Docket No.: 050108-0061

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of	:	Customer Number: 20277
	:	
Varsha CLARE, et al.	:	Confirmation Number: 6881
	:	
Application No.: 10/695,805	:	Group Art Unit: 2686
	:	
Filed: October 30, 2003	:	Examiner: Khawar IQBAL
	:	

For: OPTIMIZED NETWORK EMPLOYING SEAMLESS AND SINGLE SIGN ON CAPABILITIES FOR USERS ACCESSING DATA APPLICATIONS ON DIFFERENT NETWORKS

DECLARATION OF KEITH E. GEORGE
UNDER 37 C.F.R § 1.131

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

1.   I, Keith E. George, have been continuously employed as a patent attorney at the firm McDermott Will & Emery LLP since 1998.

2.   During my term of employment at the firm, I and other attorneys of the firm have represented the Assignee of the above-identified application, Cellco Partnership (d/b/a Verizon Wireless).

3.   Attached Exhibit 1 is a table containing time entry data which I extracted and parsed from the firm's accounting system showing attorney and paralegal time entries for services provided with regard to the above-identified application (under client number 50108 and matter number 61), up until the October 30, 2003 filing date of the above-identified application. I believe that the data for Date, TKPR Name, Client, Matter, base hours (Bs Hrs) and Narrative

contained in the table (Exhibit 1) is a true copy of data from the firm's electronic accounting system. Dates listed in the table that are prior to May 5, 2003 have been redacted.

4.   Attached Exhibit 2 contains a true copy an e-mail that I received, from Jay Hsu at Verizon Wireless, authorizing us to prepare the above-identified application. Dates shown in the e-mail document, which have been redacted, are prior to May 5, 2003.

5.   When received, the e-mail (Exhibit 2) discussed in the preceding paragraph included three attached documents.

6.   The first document attached to the e-mail (Exhibit 2) discussed in paragraph 4, file Authentication_SingleSignOn Invention.doc, was a Verizon Wireless Invention Disclosure form entitled "Authentication/Single Sign On" naming Varsha Clare, Allen Billings and Kent Hughes as inventors. Attached Exhibit 3 is a true copy of that Verizon Wireless Invention Disclosure. The second page of the Verizon Wireless Invention Disclosure form lists a conception date. That date, which has been redacted, is prior to May 5, 2003. The third page of the Verizon Wireless Invention Disclosure form identifies two detailed description documents by file names, which documents correspond to the documents discussed in paragraphs 7 and 8 below. The dates associated with those document citations, which have been redacted, are prior to May 5, 2003.

7.   The second document attached to the e-mail (Exhibit 2) discussed in paragraph 4, file Sign-on Requirements v2.0.ppt, was a document entitled "Discussion Points – Authentication and Authorization for VZW Products." Attached Exhibit 4 is a true copy of that document. This document bears no date.

8.   The third document attached to the e-mail (Exhibit 2) discussed in paragraph 4, file Data Product Authentication Briefing v2.2.ppt, was a document entitled "Authentication,

Authorization and Single Sign-on for Data Products and Services." Attached Exhibit 5 is a true copy of that document. The cover page of the document (Exhibit 5) bears a date. The date has been redacted. The date on the cover page of the "Authentication, Authorization and Single Sign-on for Data Products and Services" document (Exhibit 5) is prior to May 5, 2003.

9.   The first time entry (line # 1) in the table of data for services provided with regard to the above-identified application (Exhibit 1) is my time entry regarding my initial review and consideration of the documents (Exhibits 3-5) discussed in paragraphs 5-8 above. The date associated with that time entry, which has been redacted, is prior to May 5, 2003.

10.   After my initial review of the received documents, I assigned the application to David Tennant, for drafting.

11.   I supervised David Tennant's preparation of the above-identified application. My subsequent time entries in the table of Exhibit 1, for example, show my review and consideration of drafts of the application, prepared by David Tennant. Several time entries by David Tennant refer to me by name or by my initials KEG.

12.   The third time entry (line # 3) in the table of data for services provided with regard to the above-identified application (Exhibit 1) refers to a teleconference between David Tennant and the inventors. The redacted date of that time entry is prior to May 5, 2003.

13.   Attached Exhibit 6 is a printout of a data file containing the text of a transcript of a telephone conversation involving David Tennat, Varsha Clare, Allen Billings and Kent Hughes, which I personally recovered from the firm's electronic document management system files for this matter. Based on my own review of the directory of files for this application and the associated document creation/edit dates, I believe that attached Exhibit 6 represents a true copy

of the text of a transcript of the teleconference referred to in the preceding paragraph and that the conversation was conducted and the transcript completed prior to May 5, 2003.

14. The eleventh time entry (line # 11) in the table of data for services provided with regard to the above-identified application (Exhibit 1) refers to another teleconference between David Tennant and the inventors. The redacted date of that time entry is prior to May 5, 2003.

15. Attached Exhibit 7 is a printout of a data file containing the text of a transcript of a telephone conversation involving David Tennat, Varsha Clare, Allen Billings and Kent Hughes, which I personally recovered from the firm's electronic document management system files for this matter. Based on my own review of the directory of files for this application and the associated document creation/edit dates, I believe that attached Exhibit 7 represents a true copy of the text of a transcript of the teleconference referred to in the preceding paragraph and that the conversation was conducted and the transcript completed prior to May 5, 2003.

16. Attached Exhibit 8 contains a true copy a May 26, 2003 e-mail that I received, from David Tennat, forwarding a May 22, 2003 e-mail from inventor Allen Billings. When received, that e-mail (Exhibit 8) included two attached documents.

17. The first document attached to the May 26, 2003 e-mail (Exhibit 8) discussed in paragraph 16, file SSO – 3rd Party Authoization Requirements v.1.2.doc, was a document entitled "Single Sign-on Third Party Authorization Requirements," Version 1.2 (DRAFT), a true copy of which is attached hereto as Exhibit 9. The cover page of this first document (Exhibit 9) bears a May 21, 2003 date. Dates for two earlier versions listed on page 2 of the document (Exhibit 9), which have been redacted, are prior to May 5, 2003.

18. The second document attached to the May 26, 2003 e-mail (Exhibit 8) discussed in paragraph 16, file Single Sign-on 3rd Party Authorization Supplement.ppt, was a document

entitled "Single Sign-on Third-Party Authorization Vendor and Platform Recommendation," a true copy of which is attached hereto as Exhibit 10. The cover page of the second document (Exhibit 10) bears a May 7, 2003 date.

19.   As shown by the time entries in the table (Exhibit 1), from a date prior to May 5, 2003 until October 30, 2003, we continued work preparing the above-identified application for filing.

20.   I believe that we prepared and filed the above-identified application based on the information contained in the documents attached as Exhibits 3-7, 9 and 10 and that the application discloses and claims inventive concepts disclosed in those Exhibits.

21.   The above identified application was filed in the US Patent & Trademark Office on October 30, 2003.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

_____1/11/2006_____
Date

Keith E. George
Registration No. 34,111

Line #	Date	TKPR Name	Client	Matter	Bs Hrs	Narrative
1	▮▮▮	George, Keith E	50108	61	0.5	Initial review and consideration of invention disclosure documents.
2	▮▮▮	Tennant, David	50108	61	0.5	Meeting with Keith George regarding application.
3	▮▮▮	Tennant, David	50108	61	2.3	Reviewing invention disclosure; teleconference with inventors.
4	▮▮▮	Tennant, David	50108	61	5	Review application having related technology; review conversation with inventors; prepare notes re the same.
5	▮▮▮	Tennant, David	50108	61	3.3	Preparing background of the invention and detailed description of embodiments.
6	▮▮▮	Tennant, David	50108	61	2	Continued to draft detailed description.
7	▮▮▮	Tennant, David	50108	61	1.7	Reviewing prior art patents; continued drafting detailed description.
8	▮▮▮	Tennant, David	50108	61	5	continued drafting application.
9	▮▮▮	Tennant, David	50108	61	5	continued drafting detailed description; reviewing US patents re certain areas of technology.
10	▮▮▮	George, Keith E	50108	61	0.8	Review and consider partial draft application prepared by D. Tennant and provide comments/suggestions for completion thereof.
11	▮▮▮	Tennant, David	50108	61	3	Reviewing and considering inventor disclosure and draft application; revise; prepare for meeting with inventor Varsha Clare; teleconference with Varsha Clare and Allen Billings.
12	▮▮▮	Tennant, David	50108	61	1.5	Reviewing and considering transcribed telephone conversation with Varsha Claire and Kent Hughes; outline remarks and drafting application.
13	▮▮▮	Tennant, David	50108	61	5	Continue to draft patent application and preparing claims.
14	▮▮▮	Tennant, David	50108	61	3	Further drafting of claims and drawings.
15	▮▮▮	Tennant, David	50108	61	1	Review and revise application.
16	6/4/2003	Tennant, David	50108	61	3	Continue to revise application.
17	6/5/2003	Tennant, David	50108	61	1	Continue to revise.
18	6/11/2003	Tennant, David	50108	61	4	Continue to revise application.
19	6/12/2003	Tennant, David	50108	61	3.2	Continue to draft application.
20	6/18/2003	Tennant, David	50108	61	3.4	Dictating alternative embodiments and revise application.

#	Date	Name			Hours	Description
21	6/30/2003	Tennant, David	50108	61	10	Prepare application, claims, and drawings.
22	7/2/2003	George, Keith E	50108	61	1.6	Review and consider draft application prepared by David Tennant; and provide comments/suggestions for supplementing application.
23	7/2/2003	Tennant, David	50108	61	2.8	Final application revisions; draft claims to third-party application.
24	7/11/2003	Tennant, David	50108	61	1	Review and revise per KEG comments.
25	7/21/2003	Tennant, David	50108	61	2.2	Continue to revise application in accordance with KEG comments.
26	7/29/2003	Tennant, David	50108	61	3	Dictating application additions; review prior art regarding certain technology.
27	7/30/2003	Tennant, David	50108	61	3.5	Dictate additional detailed description and method claims.
28	7/31/2003	Tennant, David	50108	61	2	Continue to revise draft application.
29	8/1/2003	Tennant, David	50108	61	3.5	Final revisions to application; submit to Keith George for review.
30	8/5/2003	George, Keith E	50108	61	1.4	Reviewing and providing comments on second draft of utility application prepared by D. Tennant.
31	8/5/2003	Tennant, David	50108	61	2	Revise application; drafting program product and new method claims and conforming specification; final revisions and review; detailed e-mail correspondence forwarding application to the client.
32	8/26/2003	Tennant, David	50108	61	0.8	Reviewing application; conference call with Allen Billings discussing first draft of the application.
33	8/28/2003	Tennant, David	50108	61	1.5	Revise application per conversation with Allen Billings.
34	9/30/2003	Tennant, David	50108	61	4.8	Revise application description per inventor commentary, including adding new aspect of the invention.
35	10/14/2003	Tennant, David	50108	61	0.4	Further review of application; send to client.
36	10/29/2003	Tennant, David	50108	61	1.2	e-mail correspondence to/from inventors regarding final application, declaration, and assignment; prepare assignment and forward the same to the inventors; receive signed declaration and assignment; prepare instructions for paralegal for next day filing.
37	10/30/2003	Wilbourne, Mary C.	50108	61	1.5	Review, prepare and file new in-house utility application.

| 38 | 10/30/2003 | DeHart, Brigitte | 50108 | 61 | 0.5 | Reviewed new case matter |
| 39 | 10/30/2003 | Tennant, David | 50108 | 61 | 0.5 | contact inventors and Jay Hsu re assignment; prepare/review application for filing. |

To Keith George/DC/MW&E@MW&E

cc

bcc

Subject FW: Patent App - Authentication / Single Sign-On

Keith,

I am just busy not to ignore you. Please take a look at this application.
You can start the drafting if this will work.

-JH
-----Original Message-----
From: Asher, Shelly
Sent:
To: Hsu, Jay
Cc: Clare, Varsha; Billings, Allen; Hughes, Kent
Subject: Patent App - Authentication / Single Sign-On

Jay,

Please see the attached patent app and relevant documents. If you have any
questions or need additional information, please do not hesitate to contact
me.

Shelly Asher
Verizon Wireless
Ph: 925-279-6063
Fax: 925-279-6810
email: <mailto:shelly.asher@verizonwireless. com>
shelly.asher@verizonwireless.com
Send a short message to my mobile: <mailto:sasher@vtext.com>
sasher@vtext.com

- att1.htm

- Authentication_SingleSignOn Invention.doc

- Sign-on Requirements v2.0.ppt

- Data Product Authentication Briefing v2.2.ppt

- Blank Bkgrd.gif

Invention Disclosure

Please fill out the Invention Disclosure Form as completely as possible. This form must be approved by business group management, executive director or director. If you have any questions about the form, or about your invention, please contact Invention Administration Office at (908) 607-8141 or e-mail invention@verizonwireless.com. Please return the form, signed by each inventor, and witnessed, with drawings and flow charts (software inventions or processes) as appropriate to:

Verizon Wireless
Technology Development Department
Headquarters, Satellite Office
30 Independence Blvd
Warren, NJ 07059
Attn: Invention Administration Office

Invention Disclosure

Docket No.	
Business Group	
Attorney	
Disposition	

Title of Invention   Authentication / Single Sign On

Inventor 1   Varsha Clare
Full Name Including Middle Name   **Work Phone**   925-279-6038

E-mail Address   Varsha.clare@verizonwireless.com   **Citizenship**   US

Home Address   984 Gray Fox Circle, Pleasanton, CA 94566
Number and Street, City, State, ZIP Code, Country or Province

Inventor 2   Allen Billings
Full Name Including Middle Name   **Work Phone**   925-279-6592

E-mail Address   Allen.billings@verizonwireless.com   **Citizenship**   US

Home Address   8 Bernice #108, San Francisco, CA 94103
Number and Street, City, State, ZIP Code, Country or Province

Inventor 3   Kent W. Hughes
Full Name Including Middle Name   **Work Phone**   925-279-6511

E-mail Address   Kent.Hughes@verizonwireless.com   **Citizenship**   US

Home Address   5830 Ivanhoe Road, Oakland, CA 94618
Number and Street, City, State, ZIP Code, Country or Province

Inventor 4
Full Name Including Middle Name   **Work Phone**

E-mail Address   **Citizenship**

Home Address
Number and Street, City, State, ZIP Code, Country or Province

Date First Made Invention (Conception Date)   ▬▬▬▬

Engineering Reports, etc.   **Pages**   **Date**

Journals, Conference Proceedings   **Date**

Has the invention been disclosed outside Verizon Wireless?   ☒ Yes ☐ No   Date

Has the invention been demonstrated?   ☐ Yes ☒ No   Date

Has a product using the invention been shipped outside Verizon Wireless?   ☐ Yes ☒ No   Date

Was work done under a government contract?   ☐ Yes ☒ No   No.

Who is responsible for this (these) contract(s)?   Phone No.

COMMERCIAL FACTORS

Is the device or process now in production or used commercially?   ☐ Yes ☒ No

If so, date first used   Date product first sold   Model Number

If not, is use or production being considered?   When?

To which of Verizon Wireless's business or telephone operating companies would this invention be of   Network

interest?

What Verizon Wireless competitors are most likely to use this

Wireless and wireline operators.

invention?

How would use by a competitor be discovered?   Published information, direct use of service by our staff.

The information requested below may serve as the basis for a patent application, therefore be as complete and as accurate as possible. Please describe your invention on added pages to be attached hereto using the following outline as a guide.

---

1. **Abstract of the Invention —** In a few sentences, briefly describe what your invention is and what it does.

   This is a standardized process for: 1) Authentication of subscriber using services such as MMS, PTT; 2) Authorization of various service use by a subscriber, e.g., 802.11; 3) Single sign on user id, password for various services, e.g., MMS, PTT, vtext.com and automatic process of sending user id, password to applications platforms.

---

2. **Background Information —** Provide sufficient background information so that the function and novelty of your invention can be understood. What techniques prior to your invention were used to perform the function of your invention, and what are the disadvantages? What problem is solved by your invention? What are the advantages of your invention over the prior techniques?
   1. Without proper authentication, there is a possibility that MIN/MDN delivered by the client (in handset) may be altered before reaching the application platform
   2. Without single user id, password, VZW subscriber will be forced to set up and manage multiple user ids and passwords. VZW applications will need to develop user id, password in each application.

---

3. **Detailed Description —** (a) Describe the structural *and* functional operation of your invention. Use drawings, graphs, or flowcharts as needed to describe your invention. Give specific details, not just general information. Point out what improvements your invention incorporates or the superior performance which is obtained and *why* it is obtained. (b) Are there any alternative methods or different structural embodiments of your invention? Can the general idea or technique of your invention be extended to other related fields? (c) Which features are believed to be the novel features (be specific)?
   Attached Documents:
   1. **Sign On Requirements v2.0**
   2. **Data Product Authentication Briefing v2.2**

---

4. **Attach a copy of the most pertinent publications to your invention that are known to you.**

---

5. **After the disclosure is prepared, the inventors MUST sign in the spaces below. The witnesses should read and understand the disclosure and sign in the appropriate spaces below. The inventors and witnesses should initial and date each added page of disclosure.**

Inventor	Varsha Clare	**Date**
Inventor	Allen Billings	**Date**
Inventor	Kent Hughes	**Date**
Inventor		**Date**
Witnessed and Understood By		**Date**
Witnessed and Understood By		**Date**

Rev 02/01

GUIDELINES FOR INVENTION DISCLOSURES

A detailed explanation of the Invention Disclosure Form follows:

TITLE OF INVENTION

The title should be brief and descriptive. More often
than not, it will change during the drafting of the patent application.

INVENTORS

This includes all persons who may be inventors. By
law, the true inventors must be named. It is the
patent attorney's responsibility to determine proper
inventorship, which is a legal determination. The
order of names on a patent has no legal significance.

DATE FIRST MADE INVENTION

Conception Date

This item has legal significance and should
be carefully considered. Conception is the
mental formulation of a complete idea for
a product or process including a means of
practicing the invention and a utility. To
have a complete conception of a new
product, it is necessary to provide the
product, a method of preparing the product
(unless such method would be obvious) and
a utility for the product (unless such utility
would be obvious).

First Disclosure to Others

This item can also have significant legal
consequences. If there has been any
disclosure outside the company, the
date of any non-disclosure agreement or
other relevant agreement should be indicated.

COMMERCIAL FACTORS

Include any agreements with consultants or other companies
which may be relevant to the invention. Any expected or
contemplated sale, offer for sale, commercial use or third party disclosure of the invention must be reported to the
Legal Department.

ABSTRACT OF THE INVENTION

This is basically intended to be a summary. Any
useful background information should be provided.

BACKGROUND INFORMATION

List the relevant prior art retrieved in the prior art search. Inventors have an uncompromising duty of candor to the
U.S. Patent Office. Thus, if there is any question whether a document is relevant, be sure to include it in the list of
prior art. In addition, inventors have a continuing duty to bring prior art to the attention of the U.S. Patent Office
after filing the patent application. The closest prior art should be clearly distinguished from the invention. Be sure
to discuss any of your relevant pending patent applications when you consider the prior art.

DETAILED DESCRIPTION

This is the main section of the disclosure in which
the details of the invention are provided. It is
intended to provide sufficient information so that
the patent attorney understands the full scope of
the invention and can begin to draft an appropriate
patent application providing the maximum protection
possible. Points which should be addressed and
questions to consider in this section are listed below.
Attachments are generally used to provide the
necessary information in sufficient detail.

(a)   **Type of Invention:**

What is the invention? Is it a new
device, a new or improved process,
a new use of an old device, etc.
a new design, etc. Show drawings, graphs,
or flowcharts to help describe the invention.

(b)   **Utility:**

Describe how to use the invention.
What is all the possible practical
utilities?

(c)   **Unobviousness:**

What problems in the prior art are
solved by the invention? Would
the prior art direct an investigator
away from your invention? Give any
references which are contradictory
to your results. Mention any proposed
solutions tried by you or others which
failed. Are there surprising or
unexpected results or properties of
your process or device?

(d)   **Variations and Limitations:**

Discuss any variations, modifications,
substitutions, or other changes that
may be made within the scope of the
invention. The invention should be first described in the broadest generic scope contemplated (and
permitted by the prior art) and then described in terms of more preferred and most preferred way.

(e)   **Explanations:**

Set forth any explanations or theories you may have about how or why your invention functions. Although you may not know exactly why your invention functions and the patent need not contain such information, the information may be helpful to the attorney, particularly when addressing the obviousness of the invention.

SIGNATURES/APPROVALS

After the Invention Disclosure has been signed and dated by all suggested inventors, and witnessed, it should be approved by an inventor's Department Head. It is the Department Head's responsibility to approve the Invention Disclosure form as being complete in terms of (a) description, (b) value to the company and (c) names of all suggested inventors. The Invention Disclosure form is then sent to Invention Administration Office for review. The Invention Disclosure will be evaluated for filing and prioritized, taking into consideration other priorities and recommendations of management.

Discussion Points – Authentication and Authorization for VZW Products

Overview of What Product Servers and Applications Need

- Authentication

  - **Wireless Device:** Product Server needs to verify the identification of a user requesting service from a wireless device. Example products effected: WAP, PTT, MMS.

    - Required functionality: Product Server sends an originator's IP address, received in IP packet, to AAA (session database). AAA (session database) returns trusted MIN (received over R-P interface – authenticated MIN).

  - **Web Access:** Product Server needs to authenticate a user logging in for access to profile information stored on the Product Server. Products effected: PTT, vtext, Voice Portal, possibly WAP MMS or 802.11 in the future.

    - Required functionality:

      » Support Web interface for user to enter username and password

      » Provide a method for user to manage the password.

      » For a user that does not yet have a Web login password, generate a temporary password and send it to the user in an SMS message.

- Authorization. Two levels of authorization:

  - **Basic:** Product Server needs to verify that the user is authorized to use the service.

    - Required functionality: AAA returns a yes/no value to Product Server indicating whether the user (based on NAI, MDN, MIN, User ID or IP) is authorized to use the service. Example products affected: 802.11, 3rd Party Apps.

  - **Service Type:** Product Server or application has predefined service types (i.e. class of service), and needs to know which service type to use (example: Microsoft multiple bundles).

    - Required functionality: AAA performs basic authorization as described above, and returns service class or type. Example products affected: MS Multiple Bundles, 3rd Party Apps, and maybe WAP, PTT, and 802.11

verizonwireless

Requirements for Individual Applications (See previous page for descriptions)

➤ MMS

- Authentication
  - Wireless Device – yes (by MIN < -- > IP mapping)
  - Web Access – no (maybe in future)
- Authorization
  - Basic – yes
  - Service Type – no (maybe in future)

➤ Push to Talk

- Authentication
  - Wireless Device – yes (by MIN < -- > IP mapping)
  - Web Access – yes (for password management and profile access)
- Authorization
  - Basic - yes
  - Service Type - maybe

➤ 802.11

- Authentication
  - Wireless Device – yes (by NAI from roaming partner)
  - Web Access – yes (for password management only)
- Authorization
  - Basic - yes
  - Service Type - maybe

Requirements for Individual Applications

➢ **3rd Party Applications (e.g. MSN Multiple Bundles)**

- Authentication
  - Wireless Device - no
  - Web Access – no (done through VZW-MSN)
- Authorization
  - Basic - yes
  - Service Type – yes

➢ **WAP**

- Authentication
  - Wireless Device – yes (by MIN < – > IP mapping)
  - Web Access – not today
- Authorization
  - Basic - yes
  - Service Type – maybe

➢ **1X**

- Authentication
  - Wireless Device – yes (by IS835)
  - Web Access – yes (for password management only)
- Authorization
  - Basic – yes by IS835
  - Service type - no

Requirements for Centralized Single Sign-on Using AAA Server

➢ **Information: The AAA must store the following information to be used for desired functionality**

- Subscriber Identification Information
  - MIN – provisioned by MTAS
  - MDN – provisioned by MTAS
  - NAI – generated based on provisioned MDN
  - User-ID – chosen by user

- Authentication Information
  - 1X infrastructure Password – programmed into device (default today is "vzw")
  - User-defined Password – chosen and entered by user
  - Authentication keys for MIP

- Authorization Information – yes/no field provisioned by MTAS and a service type indicator (when required)
  - Services: 1X, EVDO, 802.11
  - Products: Vtext, PTT, WAP, MMS
 - 3rd Parties: MSN Multiple Bundles

➢ **Functionality**

- Queries for authentication.
  - Wireless Device: Product Server sends originator's IP address received in IP packet to AAA (session database). AAA (session database) returns MIN.
  - Web Access
    – Support Web interface for user to enter username and password and manage password
    – For a user that does not yet have a Web login password, generate a temporary password and send it to the user in an SMS message.

- Queries for authorization information.
  - Basic: Product Server sends IP address, NAI, 802.11, MDN or user ID. AAA returns yes or no to authorize.
  - Service Type: Product Server sends IP address, NAI, 802.11, MDN or user ID. AAA returns a service type indicator.

Web-Based Password Management

➤ **Currently, vtext.com has a web-based user ID, password management system.**

➤ **Two options:**

- Option 1 – TCS front-end, AAA data store

  - Expand vtext.com method to include all products and 802.11.

  - Develop a process where storage of user ID password is removed from vtext.com. The web interface will store the user ID password in the AAA data store.

- Option 2 – AAA front-end, AAA data store

  - Eliminate vtext.com user ID password method and database.

  - Develop user ID password process for AAA.
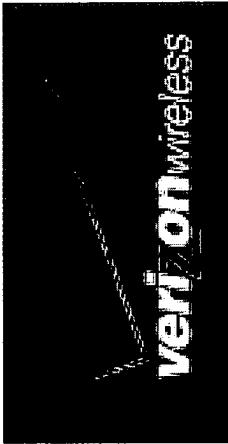
Authentication, Authorization and Single Sign-on for Data Products and Services

Network Technology Development

verizon wireless

# Authentication, Authorization and Single Sign-On: Objectives

○ Investigate a single <u>common</u> Authentication, Authorization, and Sign-on solution for Verizon Wireless products.

○ Customer Experience Objectives:

   — Allow users to sign on to any VZW product using the same username/password combination.

   — Eliminate need to enter username/password whenever it is not necessary for security.

   — Provide level of security that users can trust.

○ Network Objectives:

   — Leverage robust A-key authentication

   — Leverage AAA functionality

   — Consolidate diverse but common network solutions

   — Simplify provisioning

   — Simplify network interface requirements for Product Servers

Authentication, Authorization and Single Sign-On: Key Requirements

o Authentication of wireless device client

— HTTP based clients (WAP, PTT, MMS) present MIN as client (or subscriber identity).

— Need to assure that the MIN is not spoofed.

o Authentication of user that accesses application via web (anonymous terminal).

— Applications such as PTT and vtext require user access via web (to set up & modify profile).

· Required functionality:

· Support Web interface for user to enter username and password

· Provide a method for user to manage the password.

· For a user that does not yet have a Web login password, generate a temporary password and send it to the user in an SMS message.

— Single sign-on (user name, password) for all Verizon Wireless products including 1X, 802.11, PTT, EVDO, MMS and vtext would simplify subscriber interface.

o Authorize use of a product – 1X, 802.11, PTT, MMS, etc.

— Two types of authorizations

· Basic: Product server needs to verify that the user is authorized to use the service, e.g., 1X, 802.11, WAP.

· Service Type: In addition to basic authorization, product server needs to know service type (level of service) subscribed. Example product: Multiple Bundles.

Authentication of Wireless Device

Current

1. User launches application.
2. PDSN receives A-Key authenticated MIN over RP interface.
3. PDSN sets up data session between handset and product server. AAA and PDSN aware of MIN & IP address.
4. Product server receives MIN from the client in handset.
5. Product Servers cannot trust the MIN (may be spoofed).
6. Currently, WAP gateway uses additional key to authenticate MIN. PTT & MMS will accept MIN as given by the client.

Using AAA Session Database

1. to 5. Same as current.
6. Product Server queries session database and obtains trusted MIN to authenticate client.

Highlights:

- Session database is currently part of Ericsson Bridgewater AAA.
- Verizon Wireless has purchased this functionality.
- This is the standard process used by Product Servers in GSM.

Authentication for Web Access: vtext.com

3 TCS Username/Password Database
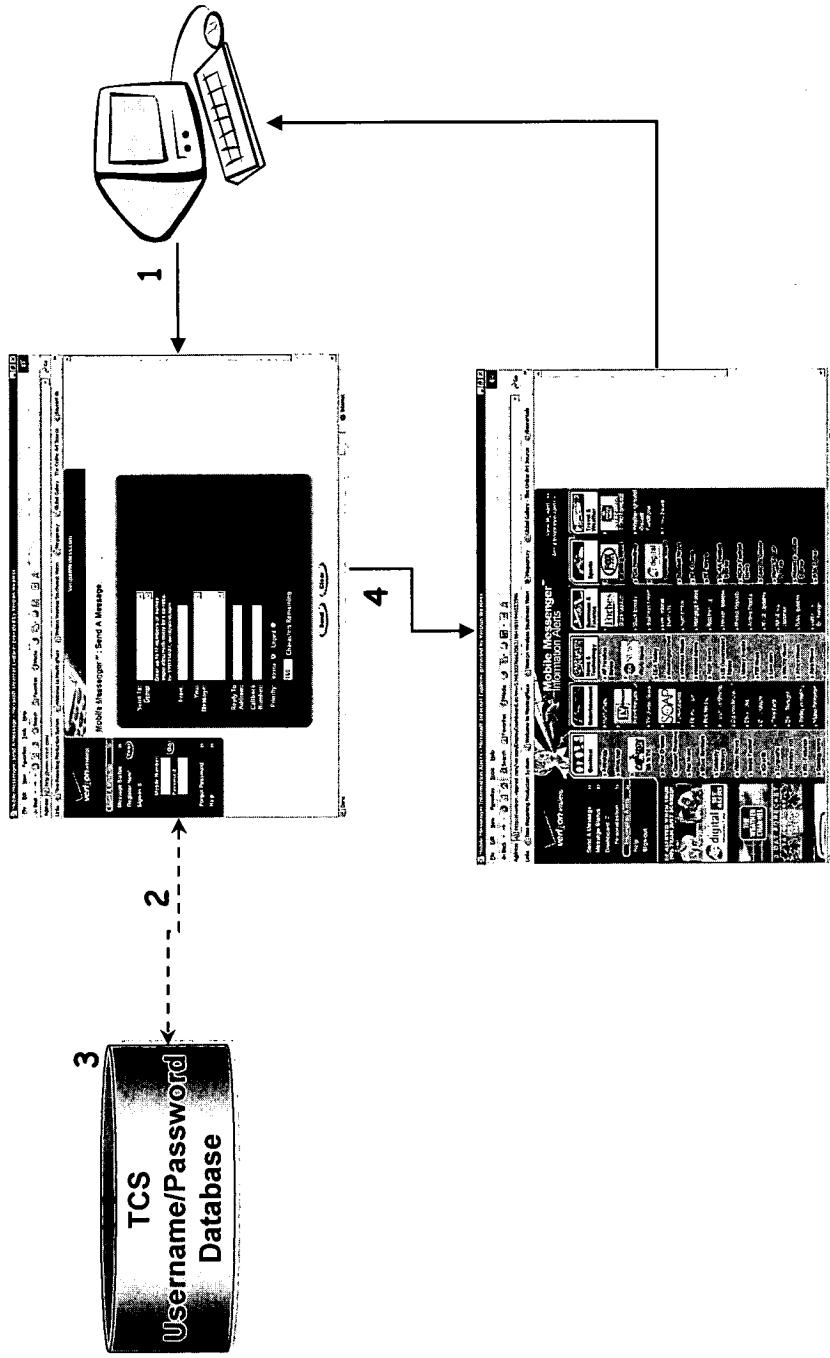
1. User goes to vtext.com and enters user name and password.
2. TCS web application provides user name password management.
3. TCS database stores user name & password.
4. TCS web application provides http redirect with user name password to Vodafone.

Authentication and Single Sign-On for Web Access: Future

AAA

Login Page

Service Select Page

Product/ WebSign-up Page

RMS

Session Database

Oracle Data Store

Radius

PDSN

IWF

MMSC

PTT

WAP

vtext

Voice Portal

PTT | VTEXT | VP

1
2
3
4
5, 6
7

Select the Service to Configure or Access
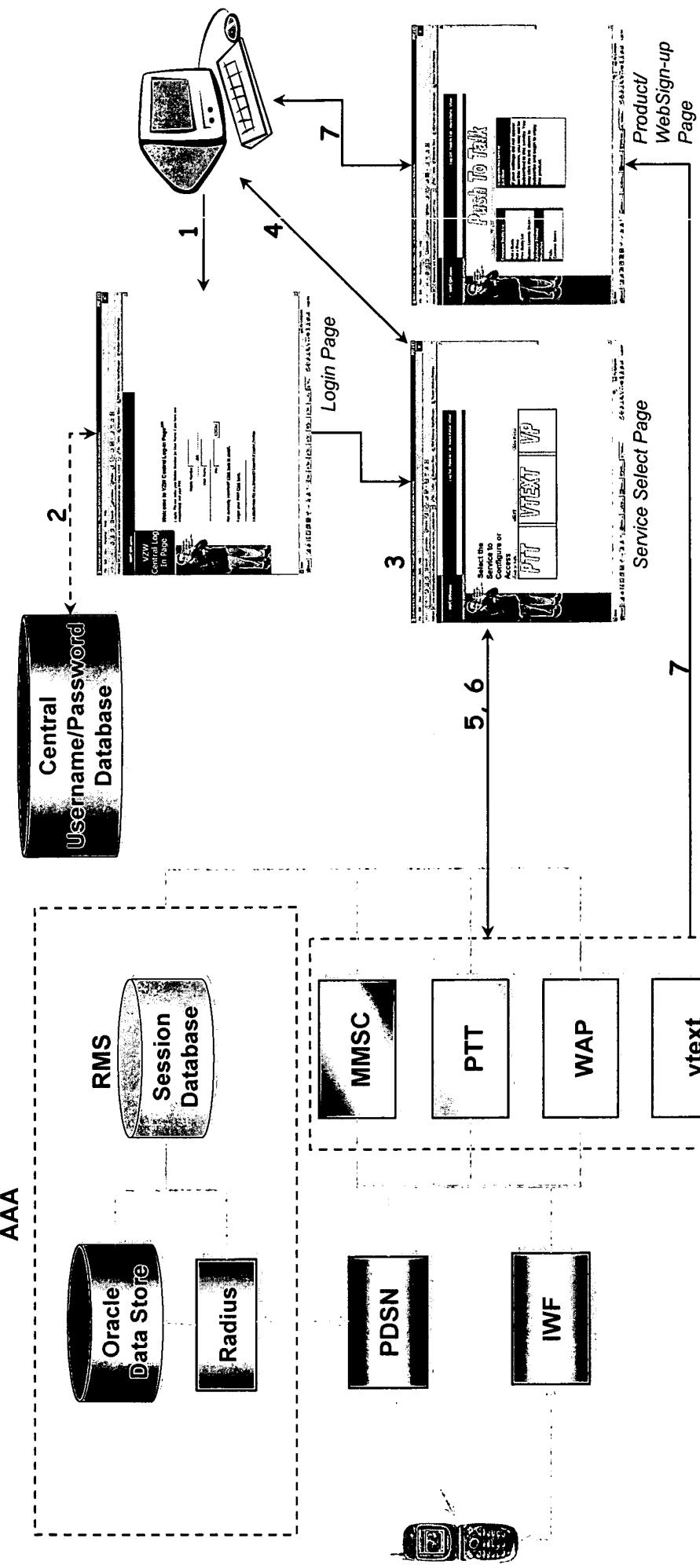
1. User links to VZW Products and enters username and password
2. Login authenticated by central database (TCS) or AAA
3. Menu of VZW products displayed
4. User selects a product
5. HTTP redirect sent with Username/password to Product Server
6. Product Server checks if user is provisioned
7. User is logged in or given opportunity to sign up for service

Highlights:

- TCS application developed for vtext.com.
- PTT application is looking at using TCS.
- TCS needs to make several changes to support PTT.
- Cannot be used for 802.11 (without AAA integration).

Central Username/Password Database

Single Sign-On: Web-Based Password Management

o Currently, vtext.com has a web-based user name, password management system.

o Two options:

- Option 1 – TCS front-end, AAA data store
  - Expand vtext.com web server to include all products, including 802.11.
  - Store the user name and password in the AAA data store.

- Option 2 – AAA front-end, AAA data store
  - Develop user name password process for AAA to support 802.11.
    - Ericsson Bridgewater AAA currently provides this functionality.
      - Need Verizon Wireless adaptation (web page design).
    - Eliminate vtext.com user name password method and database.

Authentication, Authorization and Single Sign-On: Centralized Database - Concept
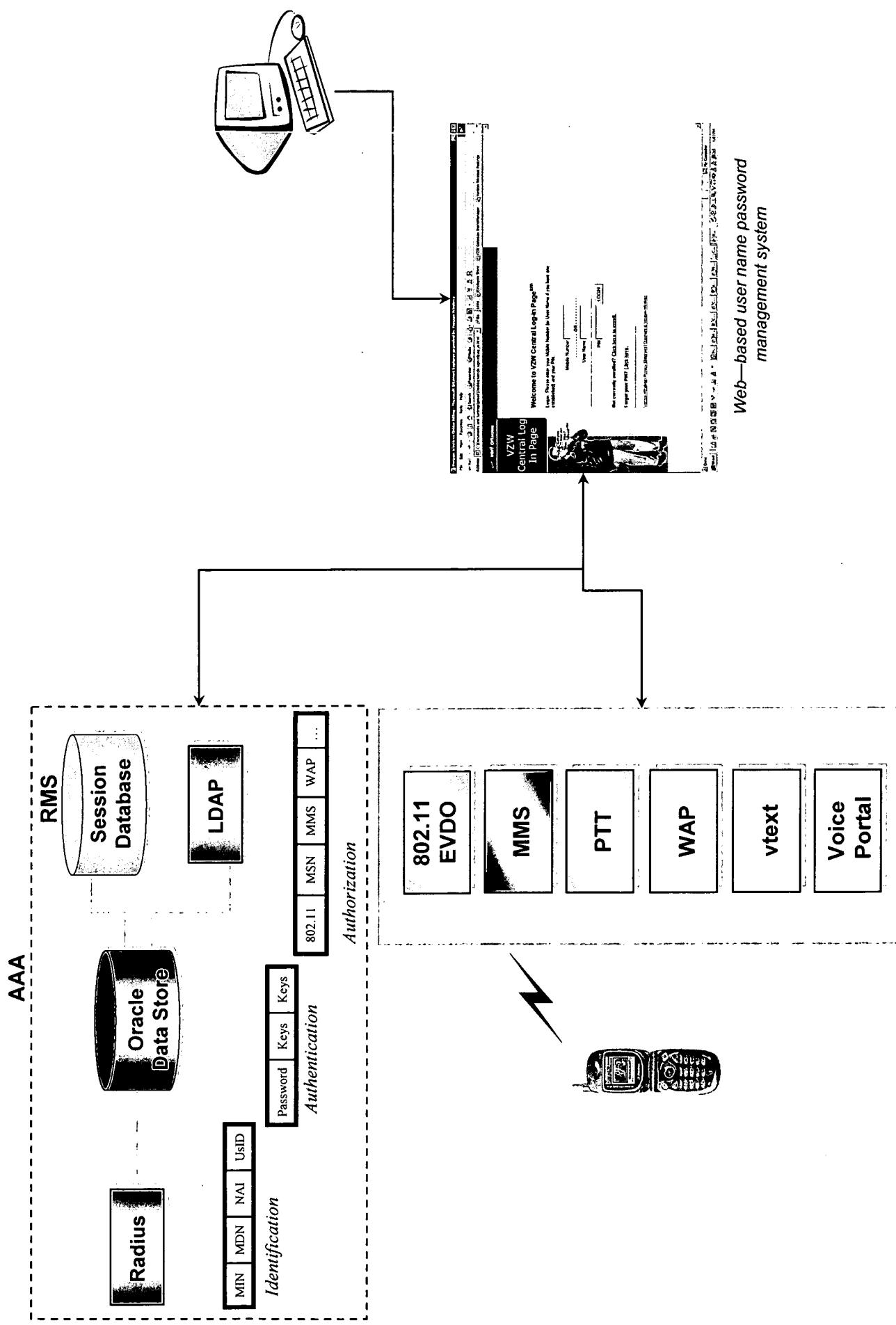
Web—based user name password management system

AAA

RMS

Session Database

LDAP

802.11	MSN	MMS	WAP	...

Authorization

Oracle Data Store©

Password	Keys	Keys

Authentication

Radius

MIN	MDN	NAI	UsID

Identification

802.11 EVDO
MMS
PTT
WAP
vtext
Voice Portal

VZW Central Log In Page

Welcome to VZW Central Log-in Page℠

Login: Please enter your Mobile Number (or User Name if one has one established) and your Pin

Mobile Number
OR
User Name
Pin
LOGIN

Not currently enrolled? Click here to enroll

I forgot your PIN? Click here.

A Few Thoughts on LDAP

o   In the future, 3rd party applications and new products may require additional data fields that are common to many applications (note: these are not authentication and authorization fields).

o   It may be preferred that these applications have LDAP interface available to the common store.

o   LDAP and AAA data store will have some common data items.

o   Ericsson-Bridgewater AAA claims to have LDAP interface available.

   —   Not clear if this requires external LDAP directory (duplicated data or access to Oracle database via LDAP protocol).

Authentication, Authorization, Single Sign-On: Highlights

○ Must Do

   — AAA Session Database for authentication of MMS, PTT, WAP clients.

   — Common user name and password for PTT, vtext.com, 802.11, 1X, EVDO.

   — AAA to authorize more than 1X.

     • 802.11

     • EVDO

○ Key Challenges

   — All of the above need Network Planning Support.

     • AAA is central to all of these functions.

     • AAA is being impacted by other key feature, e.g., 1X, Prepay Data.

○ Topics of Intense Debate

   — Role of AAA.

   — Roles and responsibilities for authentication and authorization.

   — Organization responsible for central data store.

APPENDIX

Summary of Authentication and Authorization Requirements

○ What Product Servers and Applications Need

— Authentication

- Wireless Device: Product Server needs to verify the identification of a user requesting service from a wireless device. Example products effected: WAP, PTT, MMS.

  • Required functionality: Product Server sends an originator's IP address, received in IP packet, to AAA (session database). AAA (session database) returns trusted MIN (received over R-P interface – authenticated MIN).

- Web Access: Product Server needs to authenticate a user logging in for access to profile information stored on the Product Server. Products effected: PTT, vtext, Voice Portal, possibly WAP MMS or 802.11 in the future.

  • Required functionality:

    – Support Web interface for user to enter username and password

    – Provide a method for user to manage the password.

    – For a user that does not yet have a Web login password, generate a temporary password and send it to the user in an SMS message.

— Authorization. Two levels of authorization:

- Basic: Product Server needs to verify that the user is authorized to use the service.

  • Required functionality: AAA returns a yes/no value to Product Server indicating whether the user (based on NAI, MDN, MIN, user name or IP) is authorized to use the service. Example products affected: 802.11, 3rd Party Apps.

- Service Type: Product Server or application has predefined service types (i.e. class of service), and needs to know which service type to use (example: Microsoft multiple bundles).

  • Required functionality: AAA performs basic authorization as described above, and returns service class or type. Example products affected: MS Multiple Bundles, 3rd Party Apps, and maybe WAP, PTT, and 802.11

Requirements for Individual Applications (See previous page for descriptions)

o MMS

— Authentication
  - Wireless Device – yes (by MIN < -- > IP mapping)
  - Web Access – no (maybe in future)

— Authorization
  - Basic – yes
  - Service Type – no (maybe in future)

o Push to Talk

— Authentication
  - Wireless Device – yes (by MIN < -- > IP mapping)
  - Web Access – yes (for password management and profile access)

— Authorization
  - Basic - yes
  - Service Type - maybe

o 802.11

— Authentication
  - Wireless Device – yes (by NAI from roaming partner)
  - Web Access – yes (for password management only)

— Authorization
  - Basic - yes
  - Service Type - maybe

Requirements for Individual Applications

- o 3rd Party Applications (e.g. MSN Multiple Bundles)
  - — Authentication
    - Wireless Device - no
    - Web Access – no (done through VZW-MSN)
  - — Authorization
    - Basic - yes
    - Service Type – yes

- o WAP
  - — Authentication
    - Wireless Device – yes (by MIN < -- > IP mapping)
    - Web Access – not today
  - — Authorization
    - Basic - yes
    - Service Type – maybe

- o 1X
  - — Authentication
    - Wireless Device – yes (by IS835)
    - Web Access – yes (for password management only)
  - — Authorization
    - Basic – yes by IS835
    - Service type - no

14

Requirements for Centralized Single Sign-on Using AAA Server

o Information: The AAA must store the following information to be used for desired functionality

— Subscriber Identification Information

- MIN – provisioned by MTAS
- MDN – provisioned by MTAS
- NAI – generated based on provisioned MDN
- User-ID – chosen by user

— Authentication Information

- 1X infrastructure Password – programmed into device (default today is "vzw")
- User-defined Password – chosen and entered by user
- Authentication keys for MIP

— Authorization Information – yes/no field provisioned by MTAS and a service type indicator (when required)

- Services: 1X, EVDO, 802.11
- Products: Vtext, PTT, WAP, MMS
- 3rd Parties: MSN Multiple Bundles

o Functionality

— Queries for authentication.

- Wireless Device: Product Server sends originator's IP address received in IP packet to AAA (session database). AAA (session database) returns MIN.
- Web Access
  - Support Web interface for user to enter username and password and manage password
  - For a user that does not yet have a Web login password, generate a temporary password and send it to the user in an SMS message.

— Queries for authorization information.

- Basic: Product Server sends IP address, NAI, 802.11, MDN or user name. AAA returns yes or no to authorize.
- Service Type: Product Server sends IP address, NAI, 802.11, MDN or user name. AAA returns a service type indicator.

Solution #1 – Authentication for Wireless Devices

○ Authentication for Wireless Devices

   — PROBLEM STATEMENT

      • 1X Network relies on A-key authentication to identify subscriber

      • This identification is not passed downstream to Product Servers and applications

      • Product Servers know that the user has been authorized as a valid, paying Express Network subscriber, but they don't have trusted identification of the subscriber

   — GOAL: Leverage A-key authentication to securely identify the user at the Product Servers to avoid implementing unique authentication solutions by each Product Server.

   — SOLUTION: Query into the AAA Session Database

      • Session Database holds a list of active data sessions, which can be used for subscriber identification

      • When a request for service is made, Product Server begins providing service, while making a query (in the background) to the Session Database to verify identification of the subscriber.

      • Required functionality: Product Server sends an origination IP address, received in IP packet, to AAA (session database). AAA (session database) returns trusted MIN (received over R-P interface – authenticated MIN).

      • If subscriber identification matches, service simply continues. If subscriber identification does not match, then the Product Server discontinues tears down the session.

   — STATUS: Solution is currently being implemented

      • Session Database is part of the AAA RMS, which was purchased by VZW as part of the Express Network implementation.

      • Working with Ericsson/Bridgewater to finalize specifications for the Session Database query.

      • Working with Product Server vendors to implement query capability and authentication algorithm.

Solution #2 – Authentication and Single Sign-on of Anonymous Web Users

o Authentication and Single Sign-on of anonymous Web users

  – PROBLEM STATEMENT:

    • Product Server needs to authenticate a user logging in for access to profile information stored on the Product Server.

    • Solution should utilize a single username/password among all products, and allow users to click among different product web sites without requiring re-entry of username or password.

    • Products effected: PTT, vtext, Voice Portal, possibly WAP MMS or 802.11 in the future.

  – SOLUTION

    • Today – login page and central Oracle database hosted by TCS. HTTP redirects to individual applications

    • Future – utilize capabilities of AAA server and database to store username/password along with current AAA data

    • Required functionality:

      • Support Web interface for user to enter username and password

      • Provide a method for user to manage the password.

      • For a user that does not yet have a Web login password, generate a temporary password and send it to the user in an SMS message.

  – STATUS:

    • Current solution is being implemented. Central Oracle database currently in-use for Vtext. HTTP redirects currently used for Vtext alerts. 3-4 week integration and testing each time a product is done. Web design in-process.

    • Future solution is under evaluation.

Solution #3 – Authorization: 2 Levels

○ **Basic Authorization**

  — PROBLEM STATEMENT

    • Products need to verify that the user is authorized to use the service.

    • Example products affected: 802.11, 3rd Party Apps.

  — SOLUTION

    • Include product authorization information in the AAA.

    • Products query into the AAA for authorization.

    • Required functionality: AAA returns a yes/no value to Product Server indicating whether the user (based on NAI, MDN, MIN, user name or IP) is authorized to use the service.

  — STATUS: Currently under investigation.

○ **Service Type**

  — PROBLEM STATEMENT

    • Product Server or application has predefined service types (i.e. class of service), and needs to know which service type to use (example: Microsoft multiple bundles).

    • Example products affected: 802.11, 3rd Party Apps.

  — SOLUTION

    • Include product authorization information in the AAA.

    • Products query into the AAA for authorization.

    • Required functionality: AAA returns a yes/no value to Product Server indicating whether the user (based on NAI, MDN, MIN, user name or IP) is authorized to use the service.

  — STATUS: Currently under investigation.

Verizon Wireless Online Billing - Microsoft Internet Explorer provided by Verizon Wireless

File   Edit   View   Favorites   Tools   Help

Back | Search | Favorites | Media

Address | C:\Documents and Settings\jslee1\Desktop\single sign in\Log_in.html | Go | Links | Employee Store | VZW Gateway InphoManager | Verizon Wireless Postings

verizon wireless

VZW Central Log In Page

Welcome to VZW Central Log-In Page[sm]
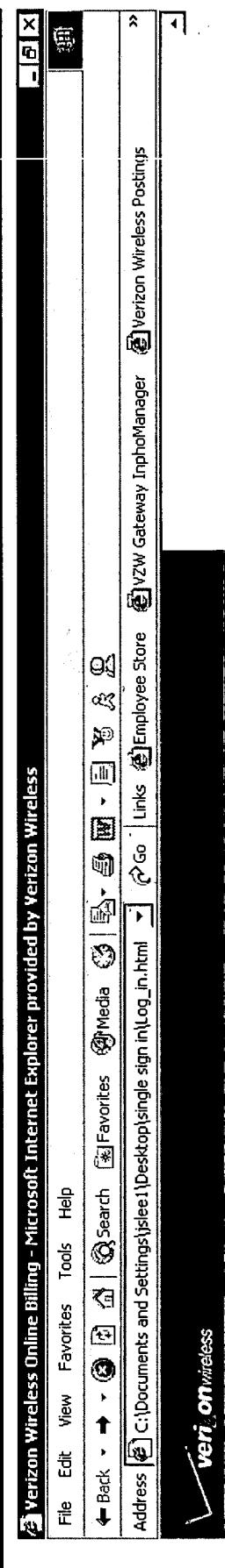
Login: Please enter your Mobile Number (or User Name if you have one established) and your PIN.

Mobile Number |_____|

- - - - - - - OR - - - - - - -

User Name |_____|

PIN |_____| LOGIN

Not currently enrolled? Click here to enroll.

Forgot your PIN? Click here.

Verizon Wireless | Privacy Statement | Copyright © Verizon Wireless
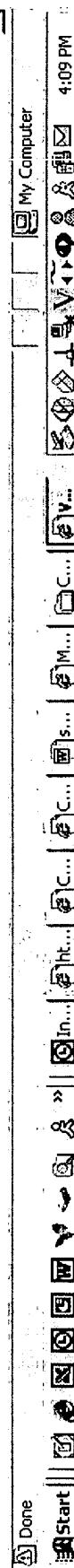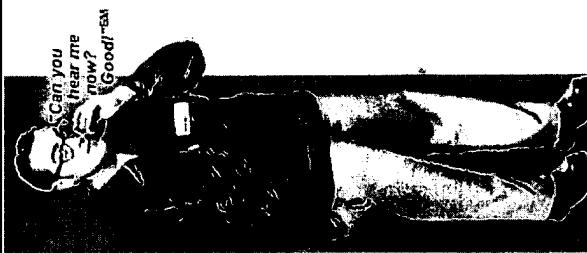
Done   My Computer

Start   4:09 PM

Welcome To Verizon Wireless - Microsoft Internet Explorer provided by Verizon Wireless

File Edit View Favorites Tools Help

Back · · | Search Favorites Media | Links

Address ents and Settings\jslee1\Desktop\single sign in\service_selection.htm Go

VZW Gateway InphoManager | Employee Store | Verizon Wireless Postings

veri_on wireless

We never stop working for you.sm

"Can you hear me now? Good!"SM

Log Out | Push to Talk | Voice Portal | VText

Select the Service to Configure or Access

Push to Talk   VTEXT   Voice Portal

PTT   VTEXT   VP

Done | My Computer

Start | Inbo... | C:\D... | Micro... | Welc... | PTT.... | Memo.... 4:28 PM

Welcome To Verizon Wireless - Microsoft Internet Explorer provided by Verizon Wireless

File   Edit   View   Favorites   Tools   Help

Back

Address   C:\Documents and Settings\jslee1\Desktop\single sign in\PTT.htm   Go   Links   Employee Store   VZW Gateway InphoManager   Verizon Wireless Postings

verizon wireless

We never stop working for you.sm

Can you hear me now? Good!sm

Push To Talk

Log Out |Push to Talk |Voice Portal |VText

Configure Buddy List

Add a Buddy
Add a Group
View Buddy List
Buddies Currently On-Line

Additional Product Information

FAQs
Customer Service

To Upgrade this Service Click Here

If your settings did not appear on this screen, you may not be subscribed to this service. You may click the link above to subscribe and begin to enjoy this product.

Done

Start   Inbox -...   C:\Docu...   Microsof...   Welco...   PTT.htm...   My Computer   4:27 PM

Welcome To Verizon Wireless - Microsoft Internet Explorer provided by Verizon Wireless

File　Edit　View　Favorites　Tools　Help

Back

Address　C:\Documents and Settings\jslee1\Desktop\single sign in\VP.htm　　Go　Links　Employee Store　VZW Gateway InphoManager　Verizon Wireless Postings

veri on wireless

We never stop working for you.℠

Can you
hear me
now?
Good!℠

Log Out | Push to Talk | Voice Portal | VText

Voice Portal

Configure Voice Services

Add an Alert
Configure Email Options
Select Preferences
Add New Content

Additional Product Information

FAQs
Customer Service

To Upgrade this Service Click Here

If your settings did not appear on this screen, you may not be subscribed to this service. You may click the link above to subscribe and begin to enjoy this product.

Done　　　　　　　　　　　　　　　　　　　　　　　　　　　My Computer

Start　　　Inbo...　C:\D...　Micro...　VP.ht...　Welc...　Welc...　4:32 PM

Welcome To Verizon Wireless - Microsoft Internet Explorer provided by Verizon Wireless

File   Edit   View   Favorites   Tools   Help

Back

Address   C:\Documents and Settings\jslee1\Desktop\single sign in\VP.htm   Go   Links   Employee Store   VZW Gateway InphoManager   Verizon Wireless Postings

veri on wireless

We never stop working for you.℠

Can you
hear me
now?
Good!℠

VText

Log Out | Push to Talk | Voice Portal | VText

Configure Voice Services

Add an Alert
Delete an Alert
Select Preferences
View Current Alerts

Additional Product Information

FAQs
Customer Service

To Upgrade this Service Click Here

If your settings did not appear on this screen, you may not be subscribed to this service. You may click the link above to subscribe and begin to enjoy this product.

Start   C:\Docu...   Inbox - ...   C:\Docu...   Microsof...   Welcom...   Welco...   My Computer   4:33 PM

DAVID TENNANT: I notice that in the invention disclosure statement it was marked that the invention has been disclosed outside of Verizon Wireless. I wanted to get some more information on that, like a date and to whom and what was disclosed.

VARSHA CLARE: Ok, I marked it because I know we all had some vendor discussions, because we are asking our vendors to develop some of this. And so that's why I made sure I marked that. We haven't given them a complete picture. The first time we gave them a complete picture was last week. But before then I think on and off in different settings we have given different pieces of information and that's why I marked it and Allen and Kent you might want to add from your perspective.

ALLEN BILLINGS: Yeah, I agree, Ericsson is really the only company that has seen anything near the full set of plans, and that was last week.

VARSHA CLARE: And another thing that I want to, one of the pieces in this is passing user id/password over http from one website to another. And that's actually one of the Verizon things that has been somewhat in place, but it was done for one application. We are extending it to multiple applications, so I might even want to add another name to the patent, assuming that one is a good key point, because we did that for one of our v-text SMS-based products first, so that probably piece was disclosed even earlier.

DAVID TENNANT: OK, well that settles, kind of, my next question, If there are any other inventors on this.

VARSHA CLARE: There may be atleast, assuming that for http direct, http-redirect, we had done that earlier with another team of some team members in my team, so I'll get from Jerry the name of the person and we'll add that person or persons.

DAVID TENNANT: Yeah, it really only depends on the scope of the claims. For example, if the claims don't cover the invention by the fourth person, then we don't need them on the application.

VARSHA CLARE: It would be, so if you could just make a note, if anything to do with http redirect with user ID/passwords then that was done by an earlier product. We kind of just packaged it and we extended it, the idea, further.

DAVID TENNANT: What's the gentleman's name?

VARSHA CLARE: Actually, I know the director's name. I don't know exactly who, Jerry Kupsch(sp?) is the director. Somebody in his team is probably what I'm going to have to bring you if you agree that, if you think that that claim is what we are going to claim.

DAVID TENNANT: Well, once we get a little further information on the invention I'll know by that time, but that's no problem to add somebody in towards the end before we file. Moving back to your disclosure to Ericsson. What exactly did you disclose and in what manner? Was it a confidential manner or was it offered as sale, for example, to enter into a contract for development of this?

ALLEN BILLINGS: There are certain pieces of this that needs to be developed on the platform that they provide us, and so in order to understand the overall picture of what we're trying to do, we presented the overall package, and that gives them the information they need to implement the individual pieces necessary to bring it all together.

DAVID TENNANT: OK

VARSHA CLARE: It's all under confidentialities and all under NDA because they're our existing vendor, and we needed them to develop a few pieces of them. We might have done, we have two, I think, two vendors involved in implementation directly, and that's Ericsson and the other one is TCS. We haven't had large conversations with TCS, but we have had small relevant conversations with TCS as well.

DAVID TENNANT: That shouldn't be a problem, as long as it's under confidential agreement and,

VARSHA CLARE: Yeah, we haven't had it in any public forum any of this discussion. It's all been within Verizon or Verizon vendors under NDA.

DAVID TENNANT: OK, good. I don't know who wants to talk first, but I normally just like to open up the floor and let you just talk about the invention, and where I usually like to start is discussing the existing technology the way the authentication and authorization is performed currently and what your pressing to do, and then we move on to the invention. So, Varsha, Allen or Kent, if any one of you will start in talking about the background and please

VARSHA CLARE: I can, and let me give it a shot first. The way this all came about is we had, like, I don't know, problems in four to five areas. They were kind of just pieces of things that were happening. We needed to support 802.11 and we didn't know how to do user ID/password, we were doing MMS and WAP gateway and we didn't know

exactly, and everybody was giving us different solutions for problems and they were like little pieces that kind of just didn't jive so we had authentication issues with how MMS and WAP gateway would work.

DAVID TENNANT: What's wrap gateway?

ALLEN BILLINGS: WAP (spells W-A-P)

DAVID TENNANT: OK, WAP. OK, yeah.

VARSHA CLARE: We were also trying to solve another product, Push To Talk, and we were getting pushed back from some of our internal parties, or the directors, who were saying "How many ID/passwords are subscribers going to have to remember?", so all of these things came at the right time, and then all of them we just kind of started thinking, "We've got to fix this", and we started thinking AAA as an answer thing. Maybe we should go take AAA and make AAA bigger and broader and then that's how this whole thing started. So until then, we were doing kind of point solutions, but not anything global and strategic. It was very much tactical, we needed to solve this problem, put a point solution in place.

DAVID TENNANT: How well do some of your competitors, like for example, Nextel, what, I'm not quite sure what they have. I know they have Push To Talk, I mean, how do they solve these problems. Do you know?

VARSHA CLARE: I don't really know for sure, but I do know one experience that I have is when Sprint launched their camera phone, just recently, and I was just sitting there watching the demo of it with some of my people and we were trying to use it, and it dawned on me, this was about a couple of months back as well, around the same time we were doing this thinking through this and David who was showing me how it was working and you could tell, in the Sprint network we went and entered user ID/password for something, and then it took us to lite surf, and then he had to enter another user ID/password to lite surf, so I know in Sprint's network you've been popped around to different places, and had to reenter the passwords.

DAVID TENNANT: OK, well that's good. Now, my understanding is that you're using a central location, the AAA, to store the authentication and password for each of your applications as well as web access as well, is that right?

VARSHA CLARE: Yeah, what we're going to do right now. and then get into more of a stepped place, the idea is we will have centralized user ID/password

for you, and then, we will have two databases, and we will synchronize the databases somehow. That's because of legacy more than anything else.

DAVID TENNANT: Yeah, alright. What stage is the development of this so far?

VARSHA CLARE: I haven't thought through all the different claims, but if you take different components, I think there's like four or five components. The http redirect to pass user ID/password from one place to another, we already have developed it and implemented it on a smaller scale. We will be broadening that. The other piece was authentication using session database to really authenticate a client. That has not been developed, or maybe some of it has been developed by Ericsson, but we are going to have them modify it, in kind of late development is what I would say. The AAA password user ID synchronization with TCS using that existing TCS process, there's already a TCS process for password management, that why I said that some of the work was existing where it sent an SMS message in a secure way and password is delivered. The synchronization piece, I would say, is in development. And, what was the fourth one, I'm missing one more, oh, the 802.11 piece, which may or may not be part of the patent, but we're adding some additional fields into the AAA to authorize and authenticate different kinds of services. Until now, we were only authenticating or authorizing 1X. We will be authorizing 802.11 and then EVDO so we would be adding some fields to the same database.

DAVID TENNANT: When is Verizon going to upgrade to 802.11, just out of curiosity.

VARSHA CLARE: First quarter next year.

DAVID TENNANT: Oh, really?

VARSHA CLARE: We hope.

DAVID TENNANT: That's good. I'm a Verizon Wireless customer, so, I might,

VARSHA CLARE: We're hoping to do something next year, Sometime next year is our plan.

DAVID TENNANT: Is that Nationally?

VARSHA CLARE: I think it's going to be, it's like, for National in 802.11 is kind of hard, it would be some selected hot spots that we would be providing service to.

DAVID TENNANT: Well, let's just move back real quick and let's just start from the beginning in terms of the invention here. I don't know if the next speaker wants to go, but essentially, you are developing the authorization for the MMS, the Push To Talk, and the 802.11.

VARSHA CLARE: And the idea is that this would be a system in place that would extend for any number of applications in any different format. That's really the main thing. The trial implementation, or first implementations, would be MMS, PTT, and 802.11. We will test out almost all our concepts by these three.

ALLEN BILLINGS: We need to differentiate between authentication, authorization, and single sign-on, because each of those are something, independent pieces. So for authentication it's authentication, it's authentication of services that go through the wireless network. For authorization, it's authorization of pretty much all the services. Then single sign-on is single sign-on of any service that requires a user ID and password.

DAVID TENNANT: Alright. And I was telling Kent earlier that I just had a chance to review the disclosure this morning, so I'm not quite familiar with the total invention and might end up giving you guys a call sometime after Thanksgiving, but I wanted to try to get as much information today so I could work over the Thanksgiving holiday, lucky me, so that I could get a draft going. Can you talk about each of the components. The authorization, how's that done or how you plan to do that, and also the authentication also the single sign-on.

VARSHA CLARE: Sure, Allen you want to do that?

ALLEN BILLINGS: Sure. So that for the, one at a time, first of all for the authentication piece. Today, we have authentication that is done on the network for 1X RTT through the AAA. And then each of the individual products are responsible for doing their own separate authentication. What we're doing is we're leveraging the authentication that occurs on our network today through the HLR to allow

DAVID TENNANT: The HLR is?

ALLEN BILLINGS: The HLR is one piece of the authentication that occurs today.

VARSHA CLARE: It's actually, maybe HLR and authentication center. They authenticate currently our subscribers. We will use that to take it through AAA, which AAA already has it, so the most secure authentication we have is HLR authentication center. So, what we are looking at doing is using that information, bringing it down,

which actually does come down, but utilizing that authenticated, when a subscriber is authenticated through HLR then we ask product servers to check, compare things with that type of authentication so now we can carry on.

ALLEN BILLINGS: So the HLR and authentication center process that is used today was developed originally for the wireless voice network, and some of the early data services, but it hasn't been extended for wireless data products, so that's part of what we're doing, is we're leveraging the authentication that occurs there to allow these individual products to find out the status of the, the authentication status that has already occurred for a given subscriber. So,

KENT HUGHES: and exactly who is starting the data session

ALLEN BILLINGS: right, so to sort of walk through the process when the user [tape ends], and then a data session is set up through approval of the AAA server. So at that point the AAA knows that the user has been authenticated to use the service and has an IP address. And at that point the user is free to access, free to get to the different applications that we have on our network, such as MMS, Push To Talk, and in the future, WAP. But those individual services do not, cannot guarantee the subscriber is who they claim they are because the authentication has already occurred and has been through a legacy system, so by the time the data and the request reach those applications, all they know is that the user is a Verizon Wireless user, but they don't know who that user is and whether it's the same user, in other words the information can be spoofed. So what those individual product servers will do is they will, when a request comes in, for example, to the Push To Talk server, requesting service, that server will begin the process of allowing service to the user, but in the background, the server will make a query into the AAA, to verify, make a query with the IP address of the subscriber to verify that the IP address belongs to the MIN that the subscriber is claiming for the connection. So, by making that query into the AAA, it basically verifies the information that has come in as a request to the server. So, it's a process of the user makes a connection, attempts to get service at the box by giving authentication information to the box, the box, the application, will then go to the AAA and verify the information that comes in. And then we're applying that same principal to all of the other products that are accessed through the wireless network as well. OK?

DAVID TENNANT: Sounds good. Now,

ALLEN BILLINGS: So that's the authentication piece. The next one is the authorization services. So, today, we have each of the applications have their own method of doing authorization. So, for example, the Push To Talk gateway, or the MMS gateway or MMSC is what it's called, they'll have their own database which lists which users have been provisioned for those services, and what we've disclosed in these plans is to move that authorization information to a common location, which is the AAA server again.

VARSHA CLARE: But on that one, just adding a couple more things, we may, as far as implementation is concerned, we may leave some authorization to the product servers depending on whatever's easiest. Because if products already do a lot more than just authorization, there's profiles and things like that then we may keep it there, but it gives us the flexibility to do simple authorization through AAA and anything more complicated, product specific, then it can go to the product server. The way this gets really interesting is the third parties. If we wanted to have like, for example, Microsoft wants to know which subscriber has subscribed to Microsoft service or what level of Microsoft service, that's where we want them to come to this AAA or the database, common database and we will tell them based on the subscriber. We will definitely want to go in that direction for the third party authorization for this mechanism. For internal products, like for 802.11, we will use this method, but for MMS we probably won't use this method because there's a lot more to be authorized and there's a lot more profile that MMS already has to do anyway.

ALLEN BILLINGS: Right, so the design is to have the flexibility to do authorization at the AAA for any of the services that we want, and the authorization will include, simply saying yes or no, the user can have service, or it can additionally indicate a particular level of service like a tiered service.

VARSHA CLARE: Or type of service

ALLEN BILLINGS: Or type of service, so it can say, for example, User A has Gold service and User B has Platinum service for this particular product. So that will allow us to authorize at different service levels for third parties off our network as well as any of the applications that ride on our network, as well as applications like 802.11, which are more of an access technology than a specific product, so it's basically a user requesting a connection as opposed to a user requesting a particular service. So, in all of those cases, the flexibility to do the authorization in one location is part of our plan. And then as far as you mention the actual implementation of that will be handled on a

7

case by case basis where we say, OK, it makes sense to do this authorization here, but in this case it doesn't.

DAVID TENNANT: Moving back to the existing setup right now, does each, like, TZT, MMS, each of those do the authorization locally?

ALLEN BILLINGS: So we actually haven't launched MMS yet, with the process that we're specifying in this patent, and they would do their own authorization.

VARSHA CLARE: And actually, this whole thing is coming about, is because we having so many new products that are data products. We haven't had to do too many of these until recently, so we haven't had to have too many product authorizations that are individually done. We had WAP gateway did some authorization, which it might continue to do some and then the next one is MTT and MMS, so they're the first applications we're getting.

ALLEN BILLINGS: And from the authorization perspective, the real power of this approach is for any authorization attempts that are coming off of our network. So for MMS, Push To Talk, and WAP, those are on our network. We're building in the flexibility to do them, but that's not where the real power is. The real power is for 802.11, where users are coming from hot spots and off network location that we don't have as much control of, and then the other area are third parties such as Microsoft where they're not on our network, but they need to come, their servers need to check with our network to see what the authorization status is for a particular subscriber.

KENT HUGHES: What currently these people are authorized for.

ALLEN BILLINGS: Right

VARSHA CLARE: And the other example of existing service is our original v-text, which is the TCS you are talking about. The v-text service we started authorizing v-text service through this database, and what we are doing is we are just using, instead of calling it v-text database it's going to be called general purpose database, that will, actually, I'm sorry it's not authorization it's user ID/password verification only, so I misspoke

ALLEN BILLINGS: Yeah, so that would be the third area that we haven't got to yet. Any other questions on the authorization piece?

DAVID TENNANT: In terms of implementing a third party authorization with the AAA now, how do you propose to do that, or just give me an idea of how you think you might implement that?

ALLEN BILLINGS: One way it could be implemented is basically, when a user requests service, they'll launch an application and be routed to the third parties server. And then that server would, similar to the authentication thing we said earlier, that server would query our network to find out the provisioning status of that user.

VARSHA CLARE: So that to add to that, one of the other things that happened during this period that helped us come up with this solution, is we were asked by our marketing group in our third party vendors to create a new database, and have LDAP interface with the database because all of the third party vendors want to dip into some databases and get Verizon specific information, but Kent was working on a project that we were going to spend, I don't know, a couple of million dollars to make that product work, and then we said why are we creating multiple databases, why not use AAA database so we have since abandoned that whole two million dollar implementation of another database and we're gonna try to centralize it in this AAA oracle database so that all the third parties that wanted to go to that new database will just, for them, this will be the database they will go to, and we will give them the LDAP interface to the database.

DAVID TENNANT: Alright.

VARSHA CLARE: This really, there is not really rocket science, in any of these things we are doing, it is really packaging.

ALLEN BILLINGS: Yeah, it's just solving a problem that's been out there, well, not really been out there, but you can

VARSHA CLARE: It's nothing brilliant, like a brand new invention, as such, but it's really

ALLEN BILLINGS: Yes it is

VARSHA CLARE: packaging, for multiple problems.

ALLEN BILLINGS: Yeah, it's piecing together a bunch of disparate parts.

DAVID TENNANT: Suppose that one of these third party services, for example, my charge for a certain feature that they might offer. Would you also be able to track that within the same database, the AAA, or how do you foresee overcoming those problems.

ALLEN BILLINGS: It depends on who's making the decision as to where the decision point is to how much the user is being charged. If the third party has stored in their database how much their charging for the different things and they're going to be billing the customer, then what they would do is query our network, actually either way it could be done this way, they would query our network and we would return to them whatever provisioning status or level or tiered service, whatever, that that subscriber has.

VARSHA CLARE: Yeah, but, the perfect example is the one that we wanted to launch with Microsoft at one point, which has been deferred for now. Microsoft would have three levels of services, the three premium services and subscribers will subscribe to one of these services. In Verizon's billing system, what we would do is we would have Microsoft dip into this database and say, "Here is a MIN, what level of service does this MIN have?" the answer would come back saying, Level 1, then Microsoft would just give them Level 1 service. Then we will bill the Level 1 service and we will give the authorization for Level 1 service to Microsoft through this process.

ALLEN BILLINGS: That way we don't need to, that way we control the provisioning on our own systems, and Microsoft just allows the different service based on what we tell them.

DAVID TENNANT: Now, moving on. You said earlier that the third aspect was the single sign-on. Correct, Allen?

ALLEN BILLINGS: Yeah, so the third aspect is the single sign-on, and essentially, that is any of the applications that require a username and password entry would use the single sign-on process and there are kind of multiple parts to this and one of them is for applications such as the setting up user preferences for MMS or Push To Talk or accessing Buddy Lists and things like that with v-text. The ability to have one username and password, and the ability to pass that password back and forth between the different applications so that once the user is logged into one, they stay logged into all the others. That's what the service is and so that is all accomplished through http redirects, which is the piece that Varsha said there would be other members of the team that would be involved in that part. So there's that aspect to it, and then there's also the aspect of actually storing that password, the password that's used on the AAA server so that applications that don't go through this whole http redirect process such as 802.11, and rely on radius authentication that needs to occur at AAA server, can use the same password. So, the scenario that we'd be looking at is a user, 802.11 will not go through the same

process as, say, logging into, for example, user preferences for Push To Talk. However, if we store the password that is used for both of those applications on the AAA [tape ends] for v-text or any of the other applications.

VARSHA CLARE: And that would be the same password we would extend to any future applications, and any future technologies, network access technologies, like, for example, we could go to EVDO, and for EVDO we would use the same user password that's already populated in this AAA.

ALLEN BILLINGS: So we had, in the past, we had two processes. We had the process of logging into an application that was authenticated against the AAA, so you would log into 1X RTT or do 802.11 and both of those in order to get access to a data connection, and then separately, we had this single sign-on process that was going on for v-text and some of the related applications, that did the redirects to other applications and whatever, but that was separate from the piece that was done through the AAA. This basically marries those two process together so that they can all use the same password.

VARSHA CLARE: And one other thing is that, our marketing group is quite interested in extending this single sign-on to everything that we do, so that in the very near future we will attempt to do the same thing with Voice Portal, we have kind of, from practical work point of view, we are just limited our current development and implementation to MMS, PTT, 802.11; but very soon after that we will start integrating Voice Portals and other products that marketing has.

DAVID TENNANT: What type of service is Voice Portal, just out of curiosity.

VARSHA CLARE: I think that's the Voice Portal project that's going on. This team hasn't been too greatly involved, but it's a third party hosted service, where you can get weather and stock quotes and all kinds of information via

KENT HUGHES: Using voice recognition

VARSHA CLARE: voice prompts rather then computer interface.

KENT HUGHES: Theoretically, you can check your email while you're driving, just by talking.

VARSHA CLARE: Anything you do with the computer, you will be able to do by voice prompts to the degree it makes sense.

11

DAVID TENNANT: That's interesting. Can you talk about or just give me a little overview on the http redirect? I'm probably gonna want to put a little information, it sounds like that will be rather important in the application.

ALLEN BILLINGS: Ok, so what happens is, when the user first, There's one database that holds the login information, or I shouldn't login information but handles the interface, the login interface for these applications, and that's done by TCS today, and as I mentioned earlier, the password will be, the password that will be used the way we've drawn up this patent is the password that is stored on the AAA, so the TCS acts as an interface with the user in order to log in based on the password that's on the AAA. So the user when they're trying to get into any of these different applications will be presented with a username and password, they'll enter that, and this server will do an authentication on the user to verify that they are who they say they are, and authorize them to access whatever service they're trying to get into. Once that occurs, they will be presented with the home page of whatever application they are trying to get into. And if they link from that application to any of the other products or services that we're offering, then each of the product servers for the applications will have a key on them and they'll use that key to encrypt the username and password and put that information in the http header and then pass that onto the next application. So the user will click, so say the user at some point is looking at v-text, they've already logged in, they click from v-text to get to, say, Push To Talk. The v-text platform will take the username and password, encrypt it, stick it in the header and send it over via a redirect to the Push To Talk platform. The Push To Talk platform then will use it's key that's stored locally to unencrypt the data and can look at the username and password and say, "OK, this is a user that I have a profile for", and bring up the user's information and deliver that web page to the user.

DAVID TENNANT: Alright. This is primarily done from a computer interface.

VARSHA CLARE: The third piece is all from a computer interface because we don't need that over the air. If we needed it, we could use it, but over the air we have much robust authentication through our HLR and authentication center by the MIN of the phone. We value MIN as the user ID, and when a MIN is passed from one place to another that is authenticated, then we know who the subscriber is. I think the key here, when we're discussing it, is we needed mechanisms to first identify a subscriber, so over the air we identify a subscriber via MIN, or we identify a subscriber by either a MIN or a user ID, and then the next one will be authenticated. So, over the air, we

authenticate the subscriber via HLR authentication mechanism, and any additional authentication we do. So we don't need to get to the password. But, if, for example, there was an application which was very sensitive and warranted and additional level of security by entering user ID/password, then we would, over the air, also use the same user ID/password and check against the same database.

ALLEN BILLINGS: So basically, the process that we described in the first step, which was authentication when going through the wireless network, because we have that in place, the process for single sign-on that we are talking about here isn't needed for those accesses.

DAVID TENNANT: What about the instance where, moving back to using your mobile handset, in the instance where one of your customers is not on your network, or you have, let's just move with that instance, if he's roaming somewhere outside of your network, and he tries to access one of the applications, how would you treat that?

VARSHA CLARE: Different. If a subscriber is roaming, the authentication happens through the roaming network. And through our HLR authentication center. So, as long as subscriber's always authenticated through our authentication center.

DAVID TENNANT: Oh, really. Through the home, from the HLR?

VARSHA CLARE: Yeah, it's always authenticated at home HLR and home authentication center. So, subscriber won't even get a service on the roaming network, unless we authorize it exactly the way we authorize it when they're in our network, actually. What exactly is not great, there are different messages and things.

ALLEN BILLINGS: Yeah, so in the first process we described when the product server, the server that's hosting the product that needs to do the authentication, when it queries the AAA database, it grabs, the AAA has a record of all the users that are connected, and authenticated, trusted information about those subscribers. It sends that information back to the server. If the user was roaming at the time, our AAA would still have that data because when the user made the connection on the roaming network, the roaming network would go into our network and say "Is it OK to give the subscriber service?" and then that information would get passed to the AAA, and it would still be available for the product server to verify.

DAVID TENNANT: Ok, good deal. I know some of the disclosure that you gave a PowerPoint presentation. Did one of you create that?

VARSHA CLARE: Yep. I think it was. The one you got was an executive presentation that we made, it was done, I think Allen and I had done most of that presentation. We have several presentations and now we have some requirements as well that detail some more of what else we need to do and I think we should have the TCS requirements out in development right now.

DAVID TENNANT: Alright. When I write the application I'm probably gonna generate or just hand draft some drawings. I'd like to be able to send it to one of you guys so that you could create your own drawing kind of like what you've done in the PowerPoint presentation. I think that's really about it for now, I'm gonna get started on it, and if I have any questions, I hope I can come back to one of you guys, if that'll be ok. Which person should I contact as my primary contact?

VARSHA CLARE: Why don't you go ahead and contact me, and then depending on how much detail we need to get done, we'll get Allen and Kent as well, when it's time to get more. As long as it's just general comments, just send it to me.

DAVID TENNANT: Moving back, it's probably going to be more of a, I don't know if you're familiar, this patent application will probably be more of a concept patent application. Since you really don't have anything concrete, a concrete working system right now. That's OK, concepts are preferred because you generally draft them very broad, and a very broad manner or claim them in a very broad manner, and, if you ever change your design or way of authenticating, for example, you can always file another application on it. Nevertheless, have you worked with anybody from this firm before? Have you worked with Keith George?

VARSHA CLARE: No I haven't, but I think some of our folks have.

DAVID TENNANT: Yeah, I will be working with Keith George on this application, so he'll probably just, FYI, review everything before it goes out to you.

VARSHA CLARE: Ok, great.

DAVID TENNANT: And, good, well I think that's really about it for now, and I will contact you, Varsha, if I have any questions.

VARSHA CLARE: Thanks a lot.

DAVID TENNANT: You guys have a nice holiday, and don't eat too much turkey.

ALLEN BILLINGS: Alright, sounds good, thank you.

14
WDC99 687263-1.050108.0061

KENT HUGHES: Bye now.

DAVID TENNANT: Bye Bye.

Client Matter 50108-061
Telephone Conversation between David Tennant,
Varsha Clair, Allan Billings and Kent Hughes.

Speaker 1: The specific implementations of the very solutions of your offering regarding the single sign on. In your disclosure you discuss primarily three different solutions. First one tells use in the HTTP Redirect, that we previously discussed. Regarding that, I wanted to find out a little bit more information on that you previously noted that you have a application pending regarding the redirect application. Are you aware of that application number? Or what firm is handling it?

Speaker 2: Did we way that?

Speaker 1: Yeah, you said you had an application directed to HTTP redirect.

Speaker 2: It was probably in a different context then because when you said application you think of an application for a patent. I think what we might have implied is application that we are developing on our network.

Speaker 1: Oh, Oh.

Speaker 2: Product. HTTP application right now running on HTTP product. What we had described in that paper, we have a drawing now.

Speaker 1: How long has that been running?

Speaker 2: Its been running for a few months. In various shapes. We had Re-text ___ redirect. Probably about a year, and then we added one more piece. Now we are making this more of a systematic approach. We're adding about three of four more now.

Speaker 1: Okay.

Speaker 2: Like between now and May we would have two more added.

Speaker 1: Okay, you said for about a year its been running?

Speaker 2: Yes. One was running for about a year?

Speaker 1: Do you know when you first started running the application?

Speaker 2: HTTP Redirect? I don't but I could find out.

Speaker 1: Yeah, the reason why I asked that question is because there is a potential bar date. If you're using the application on your website for over a year, you're barred in the U.S. and also in foreign countries. So, there might be a critical date in order to file this application in order to claim rights to the HTTP redirect application.

Speaker 2: A commercial for a while?

Speaker 1: You said you have it up and running, correct?

Speaker 2: Yeah.

Speaker 2: Are they sure that we have it up and running... commercial?

Speaker 1: Oh, is non-commercial.

Speaker 2: It is commercial? Is that the question? I'm trying to understand the process.

Speaker 1: Oh, yes. If you have it running commercial, you have up to a year to file an application on it.

Speaker 2: Okay. This may have _____ then. Maybe there is another option here. If that is done, without really too much thinking, and then we decided this approach we want to take for everything so just one. One is easier to go from A to B. But now we're going from central place like a Grand Central Station to any product that Verizon would have.

Speaker 1: Okay, before you were just doing it for V-text

Speaker 2: It was V-text _____ alert.

Speaker 3: Like a point to point solution as oppose to a ___. You know? A flexible solution that allows you to add, plug in more.

2

Speaker 1: When you say authorizing products you are also referring to I guess other products that would not be necessarily be located on the same server as V-text. Right?

Speaker 1: That's right. For example we haven't decided to do this, but we could do this between our network server to IT server which is the __Serve, where you could check your billing data. You could do the same if you wanted to.

Speaker 1: Who is the expert on HTTP redirect?

Speaker 2: In our group?

Speaker 1: Who is the inventor of it? I'd like to get a little bit more detail on the specifics.

Speaker 2: Probably Sayed or Jerry then. Probably Sayed, I can get him on.

Speaker 1: Well, I want to get a little bit more detail on the redirect process because, if we want to claim, we have various solution in this application, that would be one embodiment of course, having the AA servers as a single data store and password management system and also the other embodiment. I understand that you, Kent and Allan and Marsha are the inventors on the AA data store and password management. That's right?

Speaker 1: Okay

Speaker 2: You can have direct conversation with either Sayed or Allan you could get that too because that is the same group of people working on various functions on the single sign on. Alert system about a year or so back exactly.

Speaker 1: Before you pull one of those guys on, lets find out a little bit more information on whether or not you've had it up commercial.

Speaker 2: Okay.

Speaker 1: You know, running commercially. Once we find out that, we can go ahead and move further.

Speaker 2: I think it's a year. I'm pretty sure that it's a year. I'll find out the exact dates.

Speaker 1: Well, if it's a year, we might be able to make an argument that it was just related to V-text and another ...

Speaker 2: Its definitely not true its an embodiment we wanted to come as a company together two and half year back right?

Speaker 1: Yeah.

Speaker 2: So its more recent, but it may be more than a year, I'll find out.

Speaker 1: Alright, sounds good.

Speaker 1: Well, moving on the Solution #2. When we last spoke, you gave me a more or less topical overview of how you intended to incorporate the AA server to manage the passwords and as well, the data store. Its been a couple of months since we last spoke, so first I wanted to address whether or not you've made any approvement or started to implement into the system in anyway?

Speaker 2: Yes we are. We are actually implementing everything that is this patent, I believe, to some degree or more or less we have Triple A.

Speaker 3: Our documentation doesn't this broken up into three pieces. The documentation that we have in front of us invention disclosure and then a couple of PowerPoint presentations that have some more detail in them.

Speaker 1: Okay, I'm looking at page 17 of the PowerPoint presentation.

Speaker 2: _____ single sign on unanimous web users? Is that the page?

Speaker 1: Yes.

Speaker 3: Let me read that real quickly.

4

Speaker 2: This is what we did. We have the PCS as the single user name password. One of our servers has it for all of these applications I just listed except for Voice Portal. We haven't decided to use Voice Portal. PPT Retext, MMS, 802.11.

Speaker 1: What does TCS stand for?

Speaker 3: Telecommunications System. It's the name of the company.

Speaker 2: The company that we buy platform from. We have also taken that password and synchronized to play which is the erson product. We have pretty much done all of this right? Now, we're going to test more and we will be commercially launching in may.

Speaker 3: Under solution where it says today we've done that future we are testing preparation for launch in about a month.

Speaker 1: Okay. Can you discuss the actual specifics of the database and how you are modifying the AA server to accommodate the feature capabilities? I'll just let you go ahead and start discussing that and I'll try to stop you if I have any questions.

Speaker 3: So what is the question? Just the way that it works?

Speaker 1: Yeah, the work that it works. I mean currently the AA Server is just devoted to wireless applications.

Speaker 3: Right. So it modifies the Triple A to add a user to client password. In addition to the password that's used for 1X. Then, we built an interface. We already have the application that does the HTTP redirect hosted by TCS, which helps the database that included user name and password. So we built an interface between those two platforms to update the user name and password in the Triple A.

Speaker 1: What type of interface did you build?

5

Speaker 3: Its sort of proprietary. We developed a solution so that there's a temporary database that sits on the TCS platform, and every time there's a password change, TCS populates that database.

Speaker 1: Now, when you say password change...

Speaker 3: That's a new user, a change password, a deleted user or I guess that's it.

Speaker 1: Now would it be updated by the user itself or could it also include an update by Verizon? Say someone cancels their service.

Speaker 3: It could be either. Web interface for the customer, customer goes into the web interface and makes a password change. Then, that password change shows up into this temporary database, Triple A has a connection to the TCS platform.

Speaker 1: What type of connect?

Speaker 3: It is a Oracle Database Connection. I think its called an SQL view.

Speaker 1: Okay.

Speaker 3: Then, that connection will grab the user name and password and then delete the record from that temporary database.

Speaker 1: The AA or the application will get the user name and password from the database on the TCS platform and store it onto the AA server?

Speaker 3: Yes.

Speaker 1: Okay.

Speaker 3: Then delete the record in the temporary database.

Speaker 1: Alright.

Speaker 3: Then it will be ready for the next record.

6

Speaker 1: Okay. When you're using the HTTP Redirect, and you jump from one application to the other, its my understanding that the password information is encrypted in the header information from the webpages he originally accessed. Now when you jump from application A to B, does the HTTP redirect access the A server at all or does it only do it on that first log in occasion?

Speaker 3: Okay. So after setting up that connection that I described between TCS and Triple A, at that point we have a user name and password stored on both platforms. For the product, I'm not going to use the term application anymore. The product that use HTTP redirect, the authentication is done through TCS platform and it doesn't involve the Triple A. So the user does an authentication to get that database. <END OF TAPE 1 SIDE A>

Speaker 1: Okay.

Speaker 3: There are other products which uses Triple A server to authenticate. To begin with 802.11. For that product, the users log into a web screen and then authenticate against the Triple A database.

Speaker 1: Okay. So, with this you essentially still have the two databases for authentication separate.

Speaker 3: Yep. So the next would be to potentially eliminate the user name and password from the TCS database. When the user needs to authenticate for any product, the HTTP redirect process would use the user name and password from the Triple A.

Speaker 2: But I think we _____ separate. Its really implementation detailed because we may or may not choose to do that. Whatever is most cost efficient, easy to do, we can do it. But from user point of view, It's the same. I can imaging us having the same password duplicated into four places. Right now we have it in two places, but I could see that duplicating into the IT

7

system, I can see it duplicating to maybe Voice Portal if he choose to do something like that. So you could have it in multiple places but the process of synchronization is what we will use to keep them all in sync.

Speaker 1: Okay.

Speaker 3: So, in other words its yes. So the Triple A is the master database and the TCS acts as the front end to the user in order to manage the monitoring of that password.

Speaker 1: Okay. Keeping having a master database in terms of accessing from the web, you're always going to go through the temporary TCS database on that platform.

Speaker 2: I think the temporary database that Allan talked about, that is only for updated from synchronizing updating one database to other.

Speaker 1: Okay. Sorry maybe I misspoke.

Speaker 2: Maybe we should think of in this conversation, maybe there is no master database but a duplicated database on different platforms. On the V-text platform there's database that has subscriber identification like the phone number and user id password. The same information is duplicated in the Triple A. Triple A is used for different function than TCS is used for. Its like we have HCR Triple A to do something different and TCS to do something different. They are all different elements in the network that are used for different purposes. So that Triple A is used to make a call or provide some function to the end user then Triple A will use the user id password from Triple A. Then subscriber is doing something that doesn't effect Triple A like going to download a ring tone. It doesn't work with Triple A. Then you use the database user id password to store in the TCS database. To extend that one step further lets say we decide to synchronize this with IT password. So when you are going there to check your bill, you use the

8

same user id password but you might be checking it against the password in the IT system. But see passwords are all in sync. If one gets updated they all get updated.

Speaker 1: That leads me to my next question, what is the benefit of having the master database the AAA databases as a master base? Could you not instead use the TCS database, for example, as the master database.

Speaker 2: I don't think we should use the term master in this context because there's no such thing as a master. Each one of the databases have a different purpose.

Speaker 1: Okay.

Speaker 2: I think maybe just say the database fields or database elements are duplicated or synchronized among _____ databases _____.

Speaker 1: In terms of a password update, I'm assuming you could only do that from the web access?

Speaker 2: That's how we have designed it.

Speaker 1: Could you also implement to update your password and user name via your cell phone if you so desire?

Speaker 2: Yeah, you could do that because all it is, you would be still accessing the procedures on the TCS database. You would just give a user interface from the phone but you haven't developed it. Right now only the interface has developed it is through PC. For example, you could use your PDA to update it.

Speaker 1: Okay. That's just another consideration that we will try to incorporate in the application. Alright. Lets see here. Is there anything else that you would like to add to Solution #2? I think we've hit a lot of the topics. Now, in the application, we'll probably keep it very topical. It seems like you're using Oracle software to develop the databases and also the updates.

9

Speaker 2: That's really implementation right?

Speaker 1: I agree. That's really implementation.

Speaker 2: The concept of this is we are multiple places user id passwords are sure we keep them all in sync so that user doesn't have to remember multiple passwords and user doesn't have to enter multiple passwords.

Speaker 1: Okay. I guess I'll go to page 18 of these slides. Authorization on two different levels. Now here, you're discussing obviously authorization is little different from authentication. I was trying to determine exactly what you were at getting here in terms of what products would query into the AA server for authorization and which would not and how would the single sign on benefit this application?

Speaker 2: The product that goes through Triple A, usually the network access products. Like when you're accessing network, to use 1X network 802.11 network or EvDO network you go through Triple A.

Speaker 1: Okay.

Speaker 2: You can think of it like an access a little bit of lower level. It has to go through Triple A because its nearly part of the... Its usually coming from the cellular phone or the device through the network. The other one goes through your PC connection but you could still connect to that PCS platform through your phone. That's independent. Its not access to our network, its access has been granted and then you're doing something else on top of it.

Speaker 1: I guess you have to leave in about 5 minutes? Is that right?

Speaker 2: We could stay a few more minutes if you need too.

Speaker 1: No that's okay go ahead and talk about the Solution #3 and as far as I can tell...

10

Speaker 3: One thing on Solution #3, I think is relevant is it doesn't have to be the Triple A. It looks like that's sort of an implementation issue. We may store this information on another platform.

Speaker 2: But we are doing one right now. We are as product, putting the authorization information for 802.11 because we're launching 802.11 next month. That information for authorization is in the Triple A.

Speaker 1: Okay. But you could move it to a different platform.

Speaker 2: For 802.11 we would leave it there. Any metric access, you would leave it on the Triple A.

Speaker 1: Okay, how about for V-text or if you had different levels of V-text.

Speaker 2: For example if you choose authorize MSN Service through our network, we probably wouldn't go to Triple A, we may go to another database that synchronize with Triple A. And again that is for purely implementation, cost, performance efficiency; nothing technologically different it could be Triple A but it might be cheaper for me to put another database than Triple A.

Speaker 1: But, would you do it the same way as the authentication as we discussed prior where that you would update the Triple A with the authorization levels and update the databases on different platforms with the various authorization levels as they may change?

Speaker 2: I may put different authorization levels in different servers, like in Triple A, I may leave authorization for network access 802.11 EvDO 1X.

Speaker 1: Yeah.

Speaker 2: But, I may put another database for third parties to dip into so they don't dip into my Triple A. There may be something else I put in so that MSN and Yahoo, whoever wants to

11

authorize, can dip into that other database which is still sinked up to the the degree that is required with the rest of the databases.

Speaker 1: Well how do they do it prior to this time?

Speaker 2: Right now we don't do that. Right now we don't have third party accessing any of our network elements.

Speaker 1: Well how about for Verizon Wireless' and applications.

Speaker 2: Verizon Wireless' applications that are hosted on all the TCS platform, we will do the same as we described. MMS, Push to talk, V-text. They will all follow the same user id password, but the Verizon wireless today that are hosted by third parties, like MSN, they don't fall into the single sign on today, you have a different user id password. So MSN has a different user id password than V-text.

Speaker 1: Okay

Speaker 2: Controlled by MSN.

Speaker 3: Each product basically has to store their own authorization information.

Speaker 2: Yes, the user has to go in and create a new profile.

Speaker 1: Okay, and they usually do that from the web?

Speaker 2: They usually do that from the web, like for MSN, you just go to MSN and create your own profile.

Speaker 1: Okay.

Speaker 3: This shouldn't specify a location of where this information is being stored, it is more the implementation issues, its more the process of Verizon Wireless having some element that stores this authorization information and we allow third parties to query that information.

12

Speaker 1: Okay. How do you intend to allow third parties to query it over an Access 7 network or over a...

Speaker 2: IP network.

Speaker 1: Over an IP network?

Speaker 2: Yeah.

Speaker 1: Okay, and that would be pretty much consistent with the conventional configuration of querying. Actually let me step back, do they currently query any other applications on the network over the IP network?

Speaker 2: Third parties?

Speaker 1: Yes

Speaker 2: No

Speaker 1: No, third parties are querying anything to our networks right now, they only thing we do is we make provision, our IT system make provision for the third party databases hich required when we do something we have to go have our billing system developed an interface from billing system to the third party which we don't even do it right now. I think we don't provision anything, but that would be an alternative.

Speaker 1: Okay, now going back to Solution #1, page 16... <END OF TAPE>

Speaker 2: <BEGINNING OF TAPE #2> I think all this one does is like we have an HLR authentication.

Speaker 1: Yeah.

Speaker 2: And this one uses/capitalizes on that information. Its really kind of in some ways I think it would be like tying the HLR authentication with this authentication to make sure nobody is spoofed.

13

Speaker 1: Okay

Speaker 3: Yeah, the situation we have is that the HLR authentication helps Verizon Wireless in general are with Verizon wireless billing system, essentially, that this user is who they say they are and whether or not they can get a data connection. And then once that's done, they're done with it. That's the whole purpose of the HLR authentication today. What this does is that it leverages that authentication so that when users would go, once after they've made that connection when those users go to different Verizon Wireless products, we could verify their identify. It's sort of like a product authentication of wireless devices or authentication of wireless devices for products.

Speaker 1: Okay.

Speaker 2: One way you can think of it is when a handset reaches a product server or renter goes through MMS and says give me service, MMS conceptually goes through HLR and says here is this guy asking for the service is this valid? HLR says yes. Conceptually it exactly doesn't happen that way. Product services doesn't go through HLR, product services goes to some intermediate database that is updated by some information that came through HLR and it says this MMS client is saying his phone number is 555-1212, is this really a valid 555-1212 or somebody put a computer connected to this and then just spoofed it and put somebody else's number in it and we go and check it out and say no. If it matches through the HLR authentication or if it doesn't, if it doesn't then they don't get the service.

Speaker 1: Okay, now on that note are you proposing to incorporate AAA database with the HLR authentication?

Speaker 2: In concept, that's what it would look like. There is an extension to a Triple A database that's called session database. Session database is a real-time database of every

14

connection that goes through our 1X network. And it says, for every connection it know which telephone number is using that connection and that comes through information through HLR and the product goes to that database and just says, there are all alike connections out there and it just gives them a phone number or something and says, is there a like connection that matches this connection. If the answer, it's a good connection and if the answer is no, then it's a bad connection.

Speaker 1: Okay, I'm assuming that it performs that in the background, right?

Speaker 2: In the background.

Speaker 1: Alright, Well I guess this about it for now. It's good to clarify exactly the various methods in which you propose to utilize the databases efficiently. I will... Marsha, if you can check on that date for HTTP Redirect for me that would be wonderful.

Speaker 2: Okay.

Speaker 1: And since you are rolling this thing out in May sometime, we'll definitely have to have some kind of file prior to that time. If you can give me a rough estimate of the idea on which you are going to roll off on these various solutions, that would be great too. We'll try to get it on file at least a week prior.

Speaker 2: All of these we have rolled out in some form or the other. We're testing them and our first product is going to use all of these two products, MMS and 802.11 both of these products are launched in late-May early-June timeframe.

Speaker 1: Okay, well we'll try to get it out within April then.

Speaker 2: Yes, marketing launch date is shifting based on some other factors but the network readiness for both of these products is May.

Speaker 3: Well wonderful!

Speaker 1: Thank you for your time and I'll talk to you soon.

Speaker 1: Okay bye.

Speaker 1: Thank you, bye bye.
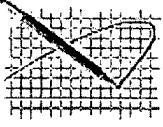
David M Tennant/DC/MW&E
05/26/2003 03:04 AM

To kgeorge@mwe.com

cc

bcc

Subject Verizon Wireless - Single Sign-on

Keith,

Please find the forwarded e-mail having an update for the single-sign on.

David M. Tennant
McDermott, Will & Emery
600 13th Street, N.W.
Washington, D.C. 20005
(tel) 202-756-8328
(fax) 202-756-8087

-----Forwarded by David M Tennant/DC/MW&E on 05/26/2003 04:05PM -----

To: dtennant@mwe.com
From: Allen.Billings@VerizonWireless.com
Date: 05/22/2003 08:29AM
cc: vxclare@NW.verizonwireless.com, JsLee1@NW.verizonwireless.com
Subject: Verizon Wireless - Single Sign-on

> David,
>
> I have attached two files with additional documentation for the Verizon
> Wireless Single Sign-on patent application. This documentation describes
> what is called "Third Party Authorization." Third Party Authorization
> allows an application platform, either on or off the VZW network, to query
> a centralized Authorization Server (the implementation of this
> functionality will be developed and loaded onto our AAA server) to
> determine whether a subscriber is allowed to use the requested
> application. The subscriber information used for Third Party
> Authorization is tied to the username/password and other data used for
> Single Sign-on, and is therefore part of the overall solution. Let me
> know if you have any questions.
>
> Allen Billings
> Verizon Wireless
> 925-279-6592
> allen.billings@VerizonWireless.com
>
> <<SSO - 3rd Party Authorization Requirements v1.2.doc>> <<Single Sign-on

SSO - 3rd Party Authorization Requirements v1.2.doc

> 3rd Party Authorization Supplement.ppt>>

Single Sign-on 3rd Party Authorization Supplement.ppt

SINGLE SIGN-ON
THIRD PARTY AUTHORIZATION REQUIREMENTS
VERSION 1.2 DRAFT
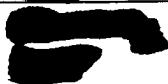
Prepared For: | Prepared By:

Technology Development
Verizon Wireless

Document Control

REVISION	ISSUED DATE	DESCRIPTION
Version 1.0		Originally created by Allen Billings
Version 1.1		Incorporated input from Jeff Lee. Added "Provisioning of Service Definitions" and "Sizing" sections.
Version 1.2	May 21, 2003	Added support for user-authentication based on user-defined password.

INTRODUCTION

This document describes the Verizon Wireless (VZW) requirements to deliver Third Party Authorization capability on a server (generically referred to as Authorization Server) installed on the VZW data network. Third Party Authorization will allow VZW applications and third party partners to query the Authorization Server for selected information, which will be used to authorize the use of applications or tiers of service for individual subscribers.

For questions on the content provided in this document please contact Allen Billings at allen.billings@VerizonWireless.com (925) 279-6592.

REQUIREMENTS

1.1 STORAGE AND CONFIGURATION OF SERVICE AUTHORIZATION INFORMATION

The Authorization Server shall store subscriber identification information and service authorization information for each individual subscriber provisioned in the server. At a minimum, the subscriber identification information shall include the user's MIN and MDN, which will be provisioned by VZW, and a user-defined password, which will be populated through a password management interface. At a minimum, the service authorization information shall include an alphanumeric, integer, or Boolean value for each service that VZW chooses to assign. There shall be no hard limit to the number of services associated with a subscriber.

The detailed format of the data must allow for flexibility in defining service authorization information and provisioning API. A final design decision on this format should be jointly made between the Authorization Server vendor and VZW, based largely on the response time and maintenance requirements for each option.

1.2 PROVISIONING OF SERVICE DEFINITIONS

The Authorization Server shall allow different VZW internal users to read, add, modify, and remove service definitions through a convenient user-interface. This interface must have multiple levels of security and user roles. Some VZW users must only be able to read the data while others may add, delete, update, and read.

1.3 USER PROVISIONING

A VZW-customized API shall be provided to allow VZW to add, modify, and remove subscriber records and subscriber services on the Authorization Server. The Authorization Server vendor shall work with VZW to define the provisioning API.

1.4 QUERIES FOR AUTHORIZATION INFORMATION

The Authorization Server shall support secure queries from specified VZW or third party product servers. Queries from product servers will include the identity of the requestor, identity of the subscriber (MIN or MDN), and the names of the requested service authorization fields or

parameters. A password may be included if user-authentication is required. The Authorization Server will send a query response to the product server, which will include MIN, MDN, user-authentication result, and the values of the requested service authorization fields or parameters. Additionally, the Authorization Server shall support queries from specified product servers that will return the values of ALL service authorization fields or parameters. The queries and responses shall be based on an industry standard format (For example a subset of current LDAP specifications). The Authorization Server vendor shall supply a detailed technical specification outlining the format of the queries and responses, and all connection and configuration information required to support the authorization queries. This specification shall be provided to any VZW vendor or partner.

1.5 PRODUCT SERVER AUTHENTICATION, CONFIGURATION, AND RIGHTS

The Authorization Server shall support a method to securely authenticate specified VZW or third party product servers. The Authorization Server will store configuration information for each individual product server, which will include, as a minimum, a list of the authorization fields or parameters that the product server is allowed to query. Each individual product server must only be allowed to query for authorization fields or parameters specified in its configuration list. The Authorization Server shall allow VZW to add, modify, and remove allowed product server configurations through a convenient user-interface.

1.6 SIZING

The Authorization Server shall be configured with adequate storage capacity to store authorization information for the entire VZW subscriber base of roughly 31 million. A subset of this subscriber base will be considered active users for the purpose of traffic calculations. A traffic model will be created to determine the transaction rate that must be supported.

REQUIREMENTS SIGNATORIES

Cellco Partnership d/b/a Verizon Wireless

By: _____

Title: _____

< Vendor >

By: _____

Title: _____

Single Sign-on
Third-Party Authorization
Vendor and Platform Recommendation

**Network Technology Development**
Draft Version 1.4
May 7, 2003

Objectives and Requirements

o Objective

- Allow VZW network elements and 3rd party partners to query an "Authorization Server" for selected information to authorize the use of applications and/or tiers of service per subscriber.

- Support username/password authentication to extend VZW Single Sign-on functionality to 3rd Parties

- Since all possible use cases have not been identified, solution should provide flexibility so that the information in the Authorization Server and associated information at the 3rd party or VZW platform can be represented differently.

o Overview of Requirements (see "*SSO - 3rd Party Authorization Requirements v1.1.doc*" for details)

- Authorization Server must support the ability to create service definitions associated with different applications. A service will contain alpha-numeric or integer fields that can be queried by an application platform or 3rd party provider

- Information within the service profiles will be accessed through a well-defined, standards-based query (such as LDAP)

  • Query will include the identity of the requestor (platform or 3rd party), the identity of the subscriber (MIN or MDN), the name of the requested field or service, and the user's password if authentication is required

  • Response will include the value of the field(s), MIN, MDN, and the authentication result (yes/no)

- New service definitions or fields can be added without further development or modification to the query format

- Authorization Server will provide a secure method to identify a 3rd Party to determine whether the 3rd party is allowed to receive the requested information

o Example Use Cases

- A 3rd party application provider of WAP services queries the Authorization Server to determine which applications the subscriber is allowed to access (pages 3 and 4)

- BREW: Users are provisioned for BREW on the Authentication Server. BREW ADS queries Authorization Server to for authorization (page 5)

WAP Example – Query for Specific Services (Using LDAP)

Authorization Server
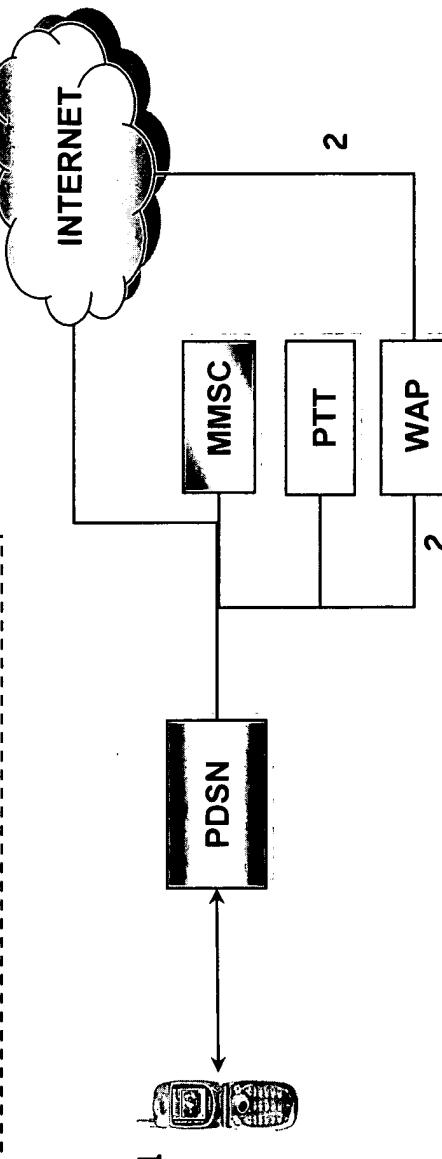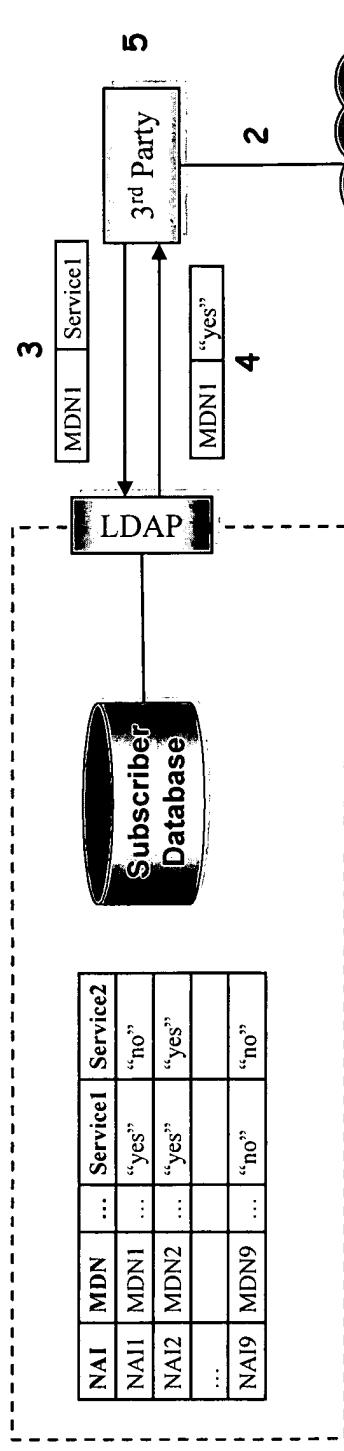
NAI	MDN	...	Service1	Service2
NAI1	MDN1	...	"yes"	"no"
NAI2	MDN2	...	"yes"	"yes"
...				
NAI9	MDN9	...	"no"	"no"

Subscriber Database

LDAP

3 | MDN1 | Service1 |

4 | MDN1 | "yes" |

5 3rd Party

2

INTERNET

2

MMSC

PTT

WAP

2

PDSN

1

1. User launches WAP browser
2. User is directed by WAP gateway, through the Internet to the 3rd party platform
3. 3rd party queries LDAP interface with MDN and requested service
4. Authorization Server returns yes/no value of service field
5. Access to application is allowed or denied by 3rd Party

WAP Example – Query for Service Level With Authentication

Authorization Server
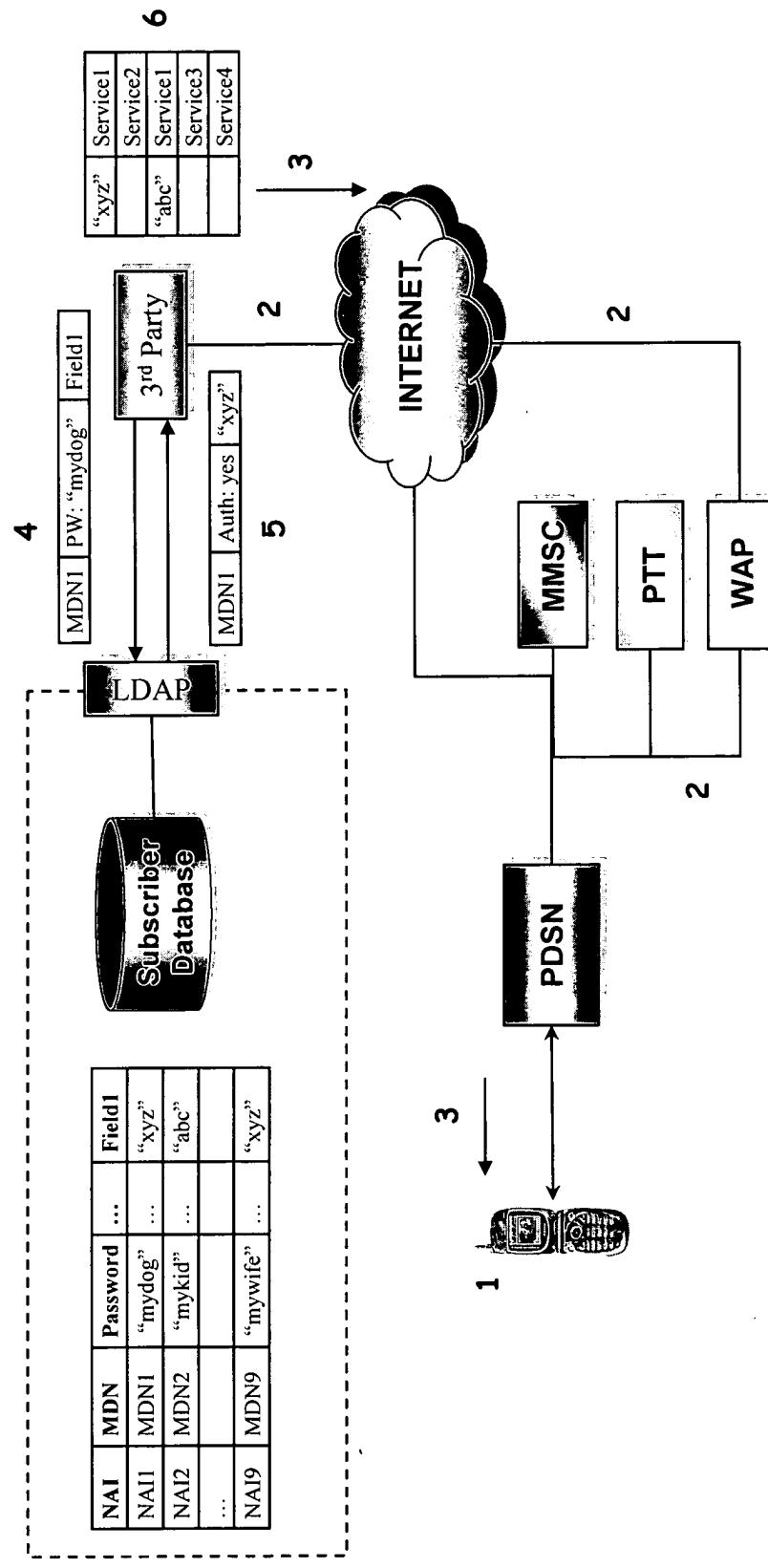
NAI	MDN	Password	...	Field1
NAI1	MDN1	"mydog"	...	"xyz"
NAI2	MDN2	"mykid"	...	"abc"
...	...			
NAI9	MDN9	"mywife"	...	"xyz"

Subscriber Database

LDAP

4	MDN1	PW: "mydog"	Field1

3rd Party

	"xyz"	Service1
		Service2
6		Service1
	"abc"	Service3
		Service4

5	MDN1	Auth: yes	"xyz"

INTERNET

MMSC

PTT

WAP

PDSN

1. User launches WAP browser

2. User is directed by WAP gateway, through the Internet to the 3rd party platform

3. 3rd party prompts user for username (MDN) and password

4. 3rd party queries LDAP interface with username MDN, password, and requested field with identifier

5. Authorization Server checks username and password and returns identifier to indicate which services are allowed

6. 3rd Party correlates identifier to appropriate service level, and associated services allowed

Authorization for BREW

Authorization Server

NAI	MDN	...	BREW	Service2
NAI1	MDN1	...	"yes"	"no"
NAI2	MDN2	...	"yes"	"yes"
...				
NAI9	MDN9	...	"no"	"no"

Subscriber Database

LDAP

3 | MDN1 | BREW

4 | MDN1 | "yes"

BREW ADS **5**

MMSC

PTT

WAP

2

PDSN

1
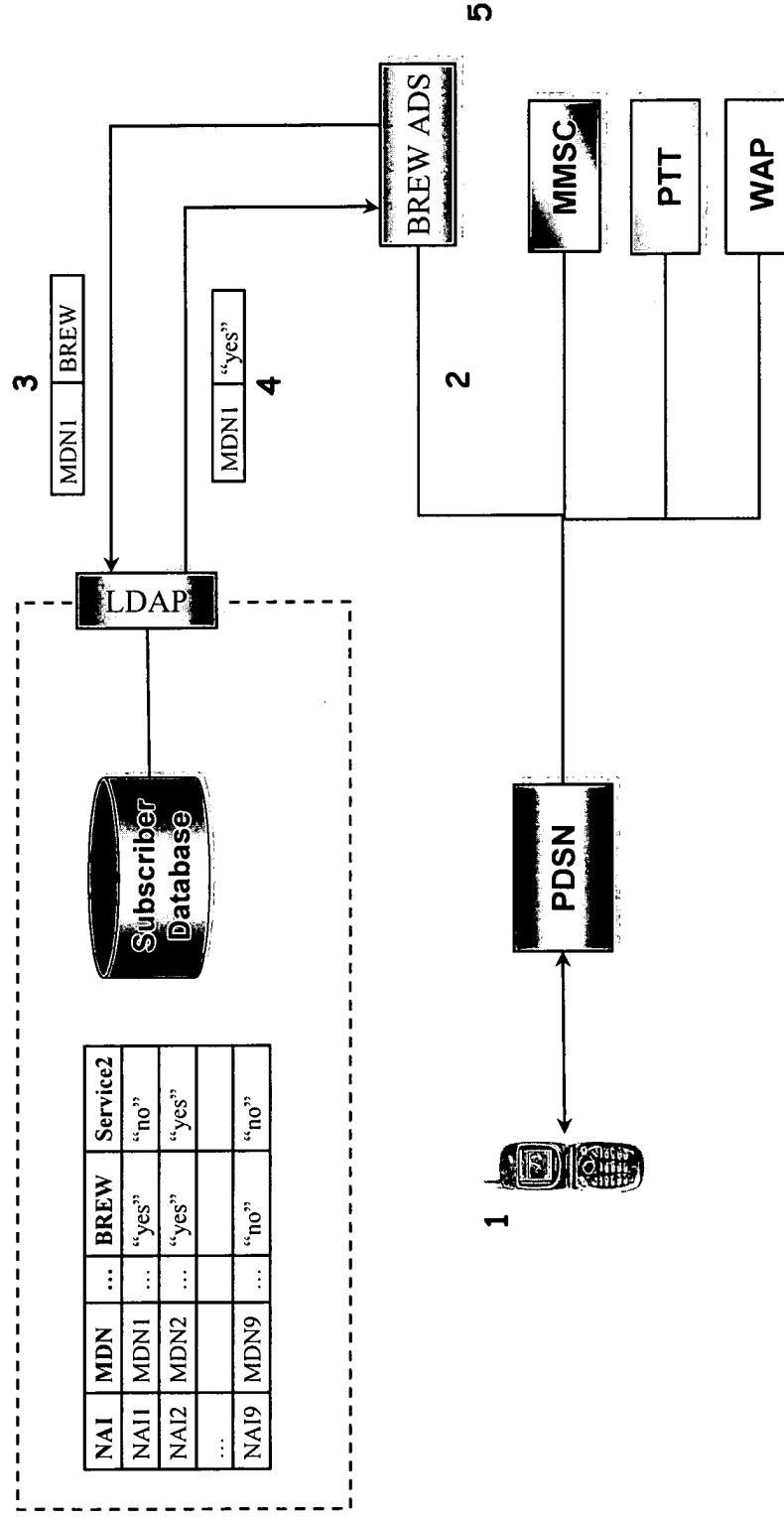
1. User launches BREW
2. User is directed to BREW ADS
3. ADS queries LDAP interface with MDN and requested service ("BREW")
4. Authorization Server returns yes/no value of service field
5. Access to BREW is allowed or denied